А. А. Торокин

# ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

*Рекомендовано Учебно-методическим советом по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности*

Москва
**«Гелиос АРВ»**
2005

УДК 004.056(075.8)
ББК 32.973.202я73-1
Т61

Рецензенты:
Заведующий кафедрой ИТЗИ Института информационных наук и безопасных технологий РГГУ, д. т. н., заслуженный деятель науки и техники РФ, профессор *А. Д. Фролов*
Заместитель декана факультета «Информационная безопасность» МИФИ, к. т. н., доцент *А. Н. Толстой*

**Торокин, Анатолий Алексеевич.**
Т61 Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. — М.: Гелиос АРВ, 2005. — 960 с.: ил. — ISBN 5-85438-140-0.

Изложены вопросы инженерно-технической защиты информации как одного из основных направлений информационной безопасности. С системных позиций рассмотрены концепция, теория, технические системы и средства, организация и методология инженерно-технической защиты информации. Структура и последовательность представления учебного материала соответствуют технологии решения слабоформализуемых задач. Для обеспечения практических занятий в приложениях приведены сценарий инженерно-технической защиты информации в кабинете руководителя организации и технические характеристики средств добывания и защиты информации.

Для студентов высших и средних учебных заведений, обучающихся по специальностям в области информационной безопасности, руководителям организаций (предприятий, учреждений), в которых существует необходимость в защите информации, и сотрудникам служб безопасности.

ББК 32.973.202я73-1

ISBN 5-85438-140-0

# Введение

*Информация* — основа жизни и деятельности человека и общества. Чем дальше продвигается наука в изучении человека, тем сложнее становится его информационная модель. Каждая клеточка нашего тела связана информационными потоками с другими его клетками и с окружающей средой. Знание глубинных информационных процессов в человеке несет большое благо и огромную угрозу. Благо, потому что возрастают возможности улучшения качества жизни человека. Но эти же возможности имеют оборотную сторону — управление человеком даже вопреки его желанию.

Традиционно считается, что когда прекращается литься кровь, наступает мир. Но в наше время такое мнение — иллюзия. Войны идут постоянно. Эти войны называются информационными. Нет нужды разрушать экологию и материальные ценности, физически уничтожать людей, когда можно, управляя человеком через информационные каналы, подчинить его себе таким образом, что это подчинение он воспримет как благо. Опасность этого оружия не только в его в массовых поражающих факторах, но и в том, что большинство людей даже не осознают факты его применения. Когда потребитель покупает в магазине товар, реклама которого постоянно мелькает на экране телевизора, то выбор часто делается не им, хотя он уверен в обратном.

Как в любой войне, имеются нападающие и обороняющие стороны. Оборона имеет два аспекта — защита от информационного воздействия и защита собственной информации. Защита собственной информации часто имеет решающее значение для исхода противостояния.

В рыночных условиях информация, кроме того, представляет товар, цена которого может существенно превышать цену самых дорогих образцов продукции. Защита ее от изменения, уничтожения и кражи представляет собой все более сложную проблему. Сложность ее обусловлена, прежде всего, тем, что в условиях рынка и информационной открытости размывается граница между свободно распространяемой и закрытой информацией. Даже предприятия, выпускающие новейшую военную технику, вынуждены по законам рынка ее рекламировать, приоткрывая тем самым завесу секретности.

Следовательно, защита информации представляет собой многоцелевую проблему, часть которой еще даже не имеет четкой постановки. Наиболее разработаны вопросы защиты информации, содержащей государственную, коммерческую и прочие тайны.

Среди ее направлений выделяют организационно-правовую, программно-аппаратную и инженерно-техническую защиту информации. Организационно-правовая защита информации осуществляется путем выполнения требований и рекомендаций правовых документов. Программно-аппаратная защита занимается обеспечением средств вычислительной техники и автоматизированных систем от несанкционированного доступа и криптографической защитой циркулирующей в них информации. Защиту информации с помощью инженерных конструкций и технических средств обеспечивает инженерно-техническая защита информации.

Инженерно-техническая защита информации объективно приобретает все больший вес. Такая тенденция обусловлена следующими причинами:

1. Развитием методов и средств добывания информации, позволяющих несанкционированно получать все больший объем информации на безопасном расстоянии от ее источников.

2. Огромными достижениями микроэлектроники, способствующими созданию технической базы для массового изготовления доступных рядовому покупателю средств нелегального добывания информации. Доступность миниатюрных и камуфлированных технических средств добывания информации превращает задачу нелегального добывания информации из уникальной и рискованной операции в прибыльный бизнес, что увеличивает число любителей легкой наживы противозаконными действиями.

3. Оснащением служебных и жилых помещений, а также в последнее время автомобилей, разнообразной электро- и радиоэлектронной аппаратурой, физические процессы в которой способствуют случайной неконтролируемой передаче (утечке) конфиденциальной информации из помещений и автомобилей.

Очевидно, что эффективная защита информации с учетом этих тенденций возможна при более широком использовании технических средств защиты.

Рассмотрению различных вопросов инженерно-технической защиты информации посвящена данная книга. При ее написании использованы материалы монографии автора «Основы инженерно-технической защиты информации» и других многочисленных открытых источников по данной проблематике. Но в данной книге предпринята попытка не только систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации, но и представить их в виде научной дисциплины. Так как стержнем любой научной дисциплины является ее теория, то наибольшее внимание в книге уделено рассмотрению теоретических основ инженерно-технической защиты информации.

Так как материалы книги имеют, прежде всего, учебную направленность, то в ней реализован структурно-системный подход к представлению знаний, который, по мнению автора, является наиболее эффективным методом изучения подобных гуманитарно-технических дисциплин. Суть его состоит в том, что изучение инженерно-технической защиты информации целесообразно проводить дедуктивным методом — от общего к частному. Для этого знания по дисциплине, образующие систему, структурируются по уровням их конкретизации. Так как объем знаний по мере их конкретизации увеличивается, то они образуют многоуровневую пирамиду. Причем на каждом уровне рассматривается горизонтальный срез всей предметной области дисциплины. Первый уровень образуют концептуальные знания по дисциплине, которые изложены в первом разделе под названием «Концепция инженерно-технической защиты информации». На следующем уровне, во втором разделе, изложены теоретические основы инженерно-технической защиты информации. Инженерные конструкции и технические средства, реализующие методы, рассматриваются на 3-м уровне (в третьем разделе книги). Основные положения по организации (организационные основы) инженерно-технической защиты информации изложены на 4-м уровне (в четвертом разделе). Методические основы инженерно-технической защиты рассмотрены на 5-м уровне (в пятом разделе).

Такое расслоение материала позволяет устранить образование множества параллельных цепочек ассоциативных связей в виде

«идея—метод—средство», которые возникают при изучении традиционно представленного учебного материала по дисциплине. Опыт говорит о том, что при традиционном представлении учебного материала знания молодого специалиста образуют систематический каталог, каждый ящик которого соответствует изучаемой теме. При решении практической задачи специалист начинает искать готовый ответ в таком каталоге. И если текущая постановка задачи не соответствует названиям на карточках ящика, то задача не решается.

Рекомендуемая же структура представления знаний заставляет проводить декомпозицию задачи по уровням и искать ответы на каждом уровне, т. е. реализовывать при решении задачи методологию системного подхода.

Такая структура приводит к некоторой избыточности за счет пересечения материала разных уровней, т. е. при изложении вопросов на более высоком уровне употребляются понятия и упоминаются вопросы, рассматриваемые на более низком уровне. Например, при изложении теории инженерно-технической защиты производится ссылка на технические средства, реализующие рассматриваемые методы. Но эта избыточность обеспечивает, во-первых, связь между разными уровнями, а во-вторых, улучшает усвоение материала.

В конце каждого раздела излагаются основные положения материала раздела. Они помогают систематизировать изученные в разделе вопросы.

Теоретические и технические основы разделены на две части, каждая из которых объединяет вопросы добывания и защиты информации. Необходимость изучения теории и средств добывания информации обусловлена тем, что специалист не в состоянии обеспечить эффективную защиту информации без знания методов и средств ее добывания.

Особенностью методических основ инженерно-технической защиты информации является то, что в них рекомендуется объединить практические и лабораторные работы единым сценарием решения сложной практической задачи по защите информации. В качестве примера такого сценария в книге рассматриваются методические вопросы защиты информации в одном из наиболее сложных объектов — кабинете руководителя организации.

Так как в связи с достаточно бурным развитием средств добывания и защиты информации их технические характеристики быстро изменяются, то данные по ним приводятся в виде приложений, которые в случае необходимости могут быть заменены на более новые.

Такое изложение материала по инженерно-технической защите информации позволяет:

- формировать в процессе обучения системное мышление, обеспечивающее системный подход к решению сложных слабоформулируемых задач и крайне необходимое специалисту в области защиты информации;
- уже в начале изучения дисциплины составить о ней общее представление, что способствует пониманию необходимости изучения последующих вопросов дисциплины;
- создавать перекрестные ассоциативные связи между знаниями разных уровней, с помощью которых эффективнее решаются нестандартные задачи по защите информации;
- формировать практические навыки по решению задач в области защиты информации.

Книга рассчитана на широкий круг читателей: студентов профессионального высшего и среднего образования в области информационной безопасности, руководителей предприятий (организаций, учреждений) и сотрудников их служб безопасности, а также читателей, интересующихся вопросами информационной безопасности.

# Раздел I. Концепция инженерно-технической защиты информации

*Концепция* — это система взглядов на что-либо [1]. Если речь идет об инженерно-технической защите информации, то ее концепция — это система взглядов на защиту информации с помощью инженерных и технических средств. С разработки концепции начинается деятельность по решению любой более или менее сложной задачи. Перед началом задуманной работы человек часто не замечает того, что его мозг создает модель будущей деятельности. Ему кажется, что решения о том, что надо делать, приходят внезапно, ниоткуда. Из ничего рождается только ничего. Иногда неразумные люди в оправдание своих ошибок повторяют фразу, что любая деятельность хуже бездеятельности, или ссылаются на приписываемые Наполеону слова, что надо ввязаться в драку, а потом видно будет. Непродуманная бурная деятельность может принести столько вреда, что ее автору лучше платить большие деньги за безделье, чем допускать к работе. Недаром одним из основополагающих принципов медицины является «не вреди». Если результаты вызывают сомнения, то лучше семь раз отмерить, прежде чем отрезать.

Но из этого совершенно не следует, что бездеятельность лучше, чем деятельность. Просто вредная деятельность хуже, чем бездеятельность. Но бездеятельность заметна и наказуема. Поэтому часто имитируют или камуфлируют деятельность. Когда, наконец, разберутся, вред непоправим. Поклонники же мировых авторитетов, дающих те или иные советы, забывают, что эти авторитеты прославились вследствие умения быстро принимать верные решения с учетом таких нюансов ситуации и среды, которые большинство людей не замечают. Таковы свойства интеллекта великих людей. Подражать им можно и нужно, но для получения таких же результатов надо иметь похожий интеллект.

Необходимыми условиями успешного решения любой задачи, в том числе и инженерно-технической защиты информации, являются постановка задачи и определение принципов ее решения. Содержание этих двух условий составляют основу концепции инженерно-технической защиты информации.

Несмотря на огромные успехи точных наук и, прежде всего, математики, далеко не всегда с ее помощью удается найти ответы на вопросы практики. Чаще постановка задачи подгоняется под известные методы решения, обеспечивающие допустимую погрешность. Однако существует очень большая группа задач, для решения которых отсутствует адекватный математический аппарат. К ним относятся задачи, результаты решения которых зависят от многих факторов, в том числе от деятельности людей. Попытки формализовать поведение или деятельность людей пока не привели к положительным результатам, за исключением достаточно простых вариантов, например деятельности операторов, реагирующих на показания приборов. Наиболее сложными являются задачи противоборства людей. Из-за невозможности формального решения такие задачи в военной сфере относят к военному искусству.

Задачи инженерно-технической защиты представляют собой задачи противоборства органов и специалистов по информационной безопасности, с одной стороны, и злоумышленников, с другой стороны. Под **злоумышленниками** в дальнейшем понимаются органы и сотрудники зарубежных спецслужб, конкуренты, криминал и любые другие люди, которые незаконным путем пытаются добыть, изменить или уничтожить информацию законных владельцев или пользователей.

Задачи, не имеющие формальных методов решения, называются неформальными, корректнее — **слабоформализуемыми**. Так как основу методологии решения слабоформализуемых задач составляют системный подход и системный анализ, то для понимания концепции инженерно-технической защиты информации необходимо понять сущность системного подхода к защите информации.

# Глава 1. Системный подход к инженерно-технической защите информации

## 1.1. Основные положения системного подхода к инженерно-технической защите информации

Слабоформализуемые задачи, к которым относится большинство задач инженерно-технической защиты, характеризуются следующими основными особенностями:

- наличием большого числа факторов, влияющих на эффективность решения задачи;
- отсутствием количественных достоверных исходных данных об этих факторах;
- отсутствием формальных (математических) методов получения оптимальных результатов решения слабоформализованных задач по совокупности исходных данных.

Эти особенности исключают возможность формального получения оптимального (наилучшего) результата решения задачи. Но даже формальный аппарат при недостоверных исходных данных не гарантирует получение точного результата. Как писал известный русский математик, механик и кораблестроитель А. Н. Крылов, «точность результатов не может быть выше точности исходных данных».

Слабоформализуемые задачи наиболее часто приходится решать на практике, в том числе при решении бытовых вопросов. Даже покупка товара сопровождается предварительными размышлениями и сбором информации о потребительских свойствах аналогичных товаров и их стоимости у разных производителей. Решение о покупке принимается на основе подсознательного анализа множества факторов, влияние которых на принятие решения часто не осознается и интегрально интерпретируется как «понравилось». Несмотря на огромные достижения науки, число проблем и задач, которые удается свести к формальным и решить строго математически, существенно меньше, чем не имеющих такого решения.

Слабоформализуемые задачи решаются в основном эвристическими методами. Однако эти методы не обеспечивают получе-

ние оптимального результата, а определяют область рациональных решений, т. е. тех, которые с определенными допусками соответствуют постановке задачи. Как правило, задача имеет несколько рациональных решений, которые в пространстве результатов образуют область, внутри которой расположено оптимальное решение.

Эвристические методы реализуют на подсознательном уровне знания и опыт специалистов. Подсознательный уровень на современном этапе развития биологической и психологической наук пока представляет собой «черный ящик», алгоритм работы которого неизвестен. Специалисты по психоанализу пытаются по отдельным проявлениям бессознательного на сознательном уровне выявить психические болезни пациентов, причины которых кроются в неосознаваемых психических травмах в предшествующие годы. Тем не менее эвристические методы решения (на основе «здравого смысла») слабоформализуемых задач часто обеспечивают более точные результаты, чем формальные на основе грубых математических моделей или при недостоверных и недостаточных исходных данных.

Однако возможности эвристических методов имеют ограничения, определяемые числом учитываемых при решении задачи факторов влияния. В силу малого объема у человека оперативной памяти количество учитываемых факторов невелико и составляет 5–9. Только отдельные выдающиеся личности способны интуитивно учитывать большее количество факторов, в силу чего принимаемые ими решения более эффективны, чем решения человека со средними способностями. В силу этих же ограничений должностные лица, которым приходится оперативно решать многофакторные задачи, имеют помощников, которые готовят им информацию в сжатом систематизированном виде.

Если число факторов влияния велико, что имеет место при решении задач инженерно-технической защиты информации, то точность эвристических методов низка. В общем случае задачи инженерно-технической защиты информации характеризуются большим количеством и многообразием факторов, влияющих на результат решения, причем это влияние часто не удается однозначно выявить и строго описать. К ним, в первую очередь, относятся задачи, результаты решения которых зависят от людей. Только в

отдельных простейших случаях удается однозначно и формально описать реакции человека на внешние воздействия. В большинстве других вариантов сделать это не удается. Однако из этого утверждения не следует, что организация эффективной защиты информации зависит исключительно от искусства специалистов по защите информации. Человечеством накоплен достаточно большой опыт по решению слабоформализуемых проблем.

Решение любых задач производится на основе моделей исследуемых объектов и процессов. Решаемая задача или проблема представляет собой разницу между реальным объектом или процессом и тем, что надо достигнуть или получить. Наиболее универсальной моделью любого объекта или процесса является представление его в виде системы. **Системный подход — это исследование объекта или процесса с помощью модели, называемой системой**.

Этот подход предусматривает самый высокий уровень описания объекта исследования — системный. Самым низким уровнем является уровень описания параметров объекта — параметрический. Между ними располагаются структурный и функциональный уровни.

Сущность системного подхода состоит в следующем:

- совокупность сил и средств, обеспечивающих решение задачи, представляется в виде модели, называемой системой;
- система описывается совокупностью параметров;
- любая система рассматривается как подсистема более сложной системы, влияющей на структуру и функционирование рассматриваемой;
- любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных оснований;
- при анализе системы необходим учет внешних и внутренних влияющих факторов, принятие решений на основе части из них без рассмотрения остальных может привести к неверным результатам;
- свойства системы превышают сумму свойств ее элементов за счет качественно новых свойств, отсутствующих у ее элементов — системных свойств.

Совокупность элементов образует систему, когда у них появляются общие цели. Если представить цели элементов в виде векторов, то векторы целей элементов простой совокупности (набора элементов) ориентированы произвольно. При сложении векторов результирующий вектор набора элементов не будет существенно отличаться от векторов элементов. Однако если векторы целей элементов ориентированы в одном направлении, то результирующий вектор будет существенно отличаться от векторов элементов. В этом случае набор элементов трансформируется в систему с дополнительными возможностями. Например, толпа людей на улице ведет себя спокойно до тех пор, пока не найдется оратор и не сблизит цели собравшихся людей. Толпа может преобразоваться временно в систему с ориентацией суммарного вектора целей как на добрые дела, так и на разрушение. Способность пламенных ораторов изменить ориентацию целей слушающих их людей и повести за собой писатели красиво назвали умением «зажечь сердца» людей. По этой же причине руководитель, назначенный или выбранный на высокий пост, собирает свою команду единомышленников, т. е. людей с одинаковой ориентацией векторов целей. Если это ему не удается, то результирующий вектор целей его аппарата возрастает несущественно, так как складываются лишь проекции целей, величина которых определяется лишь формальным выполнением сотрудниками аппарата своих функциональных обязанностей.

Важнейшим отличием системы от набора элементов является то, что система обладает свойствами, отсутствующими у ее элементов. Традиционный несистемный подход предполагает, что свойства объекта или субъекта есть совокупность свойств его частей. Примером традиционного подхода могут служить пока преобладающие в официальной медицине методы диагностики и лечения болезней человека по результатам исследования отдельных его органов. Человек к старости, после прохождения многочисленных кабинетов узкоспециализированных врачей, «приобретает» такой букет болезней, что побочный вред от назначенных многочисленных лекарств может превысить пользу от них. Человека нельзя делить на части без учета информационных, химических, электромагнитных, электрических связей между его органами и даже клетками, лечить надо не отдельные болезни, а человека в целом. Но человек

как система очень сложен. Основная проблема современной медицины состоит в противоречии между необходимостью лечения человека как единого целого и ограниченностью медицинских знаний о нем врача. Консерватизм методов лечения традиционной медицины привел к тому, что нишу системных свойств человека заполняют знахари, экстрасенсы, так называемые народные целители и другие «самородки», заряжающие энергией зубные пасты и газеты. Следует отметить, что восточная философия, в том числе и медицина, характеризуется более целостным подходом к миру, чем западная. Иероглифы, каждый из которых отображает целые понятия языка, являются примером такого подхода. Конечно, учащимся японской, корейской и китайской школ труднее запомнить несколько тысяч иероглифов, чем тридцать букв алфавита, но при изучении иероглифов уже в раннем возрасте развивается дедуктивное мышление, которое в дальнейшем способствует формированию системного мышления специалиста. Отчасти этим можно объяснить огромные успехи, например, Японии и Северной Кореи в производстве высокотехнологичной продукции.

Примером системного свойства является сознание человека, которое отсутствует у его частей. Мыслительные способности автономно функционирующего мозга как органа обработки и хранения информации и мозга в теле человека существенно отличаются. Это утверждение подтверждается соответствующими опытами: у человека, изолированного от внешних воздействий (с закрытыми глазами и ушами, помещенного в бассейн с жидкостью, плотность которой равна плотности его тела), через некоторое время возникают галлюцинации, а через более продолжительное время проявляются симптомы психического расстройства. Это можно объяснить влиянием расхождения между текущей моделью мира, которая постоянно создается в мозгу на основе информации от всех рецепторов тела человека, и эталонной, сформировавшейся в течение предыдущей жизни человека. Когда прекращается поток данных от рецепторов, то текущая модель деформируется, подсознание не может найти алгоритм сохраняющего здоровье и жизнь поведения, происходит так называемая «сшибка», приводящая к психическому расстройству. По этой же причине «теряется» человек, попадающий в незнакомую обстановку.

Эффективность реализации системного подхода на практике зависит от умения специалиста выявлять и объективно анализировать все многообразие факторов и связей достаточно сложного объекта исследования, каким является, например, организация как объект защиты. Необходимым условием такого умения является наличие у специалиста так называемого **системного мышления**, формируемого в результате соответствующего обучения и практики решения слабоформализуемых задач. **Системное мышление — это форма мышления, характеризующая способность человека на бессознательном уровне решать задачи дедуктивным методом.** Эти методы применительно к инженерно-технической защите информации предусматривают:

- четкую постановку задачи, включающую определение тематических вопросов защищаемой информации и ее источников как объектов защиты, выявление угроз этой информации и формулирование целей и задач защиты информации;
- разработку принципов и путей решения задачи;
- разработку методов решения задач;
- создание программного, технического и методического обеспечения решения задачи.

Системное мышление — важнейшее качество не только специалиста по защите информации, но и любого организатора и руководителя. Если руководитель не может быстро выявить факторы, влияющие на то или иное решение, и оценить их вес, то неучтенные или необоснованно отброшенные факторы постоянно будут о себе напоминать. Такой руководитель превращается в борца с им же создаваемыми проблемами.

Если системный поход характеризует концептуальные взгляды на пути решения слабоформализуемых задач, то основу их решения составляет системный анализ.

**Системный анализ предусматривает применение комплекса методов, методик и процедур, позволяющих выработать в результате анализа модели системы рациональные рекомендации по решению проблем системы.** Математическим обеспечением системного анализа является аппарат исследования операций. Исследование операций представляет собой комплекс научных методов для решения задач эффективного управления организацион-

ными системами, в которых основным элементом является человек. Один из создателей аппарата исследования операций Т. Саати определил его как «искусство давать плохие ответы на те практические вопросы, на которые даются еще худшие ответы другими методами». Следует сразу оговориться, что при решении слабоформализуемых задач методами системного анализа в большинстве случаев удается найти только область рациональных решений, внутри которой находится наилучший (оптимальный) для конкретных исходных данных результат.

Системный подход и системный анализ составляют основу теории систем. Теория систем зародилась в 30-е годы. В годы Второй мировой войны корпорация «Ренд корпорэшен» разработала методологию системных исследований, а в 50-е годы теория систем сформировалась как самостоятельное направление. В 50-е годы в США было организовано «Общество исследований в области общей теории систем». Его организаторами являются специалисты по математическим проблемам в области системотехники и психологии Л. Берталанфи, Р. Жерар и А. Рапопорт, К. Боулдинг. С 1956 г. «Общество ...» издает под редакцией Берталанфи и Рапопорта ежегодники «General System». В 1959 г. при Кейсовском технологическом институте (США) создан «Центр системных исследований». Корпорация «International Business Mashines Corporation» в 1963 г. организовала Институт системных исследований.

Созданию и развитию теории систем способствовали труды русских ученых В. И. Вернадского, А. А. Богданова, Л. С. Выготского, Г. С. Поспелова, Н. П. Бусленко, В. Н. Садовского, Н. П. Федоренко и других. С 1969 года в России издается ежегодник «Системные исследования», в 1976 году основан в Москве научно-исследовательский институт системных исследований РАН (НИИСИ).

В соответствии с требованиями системного подхода совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности информации, образует **систему защиты информации**. Такими элементами являются люди, инженерные конструкции и технические средства, обеспечивающие защиту информации независимо от их принадлежности к другим системам. Ядро системы защиты образуют силы и средства, основными функциями которых является обеспечение ин-

формационной безопасности. Однако они составляют лишь часть сил и средств системы защиты информации. Например, в систему защиты информации входят не только структурные подразделения (служба безопасности, отдел режима и секретности, 1-й отдел и др.), предназначенные для защиты информации, но все сотрудники организации, обязанные в меру своей ответственности обеспечивать защиту информации. Следовательно, они также являются элементами системы защиты информации организации. И если какой-либо сотрудник организации нарушит правила обращения с секретными документами, то возможен огромный ущерб, несмотря на безупречную работу других элементов системы защиты. Следовательно, структура (элементы и их взаимосвязь) системы защиты информации государства, ведомства, организации пронизывает структуру государства, ведомства, организации.

Для системы защиты информации очень трудно точно указать места входов и выходов. Входами любой системы являются силы и воздействия, изменяющие состояние системы. Такими силами и воздействиями являются угрозы. Угрозы могут быть внутренними и внешними, в том числе такие трудно локализуемые как слабая правовая дисциплина сотрудников, некачественная эксплуатация средств обработки информации или наличие в помещении радио и электрических приборов, побочные физические процессы в которых способствуют несанкционированному распространению защищаемой информации. Источниками угроз могут быть злоумышленники, технические средства внутри организации, сотрудники организации, внутренние и внешние поля, стихийные силы и т. д.

Выходы системы представляют собой реакцию системы на входы. Выходами системы являются меры по защите информации. Однако локализовать в пространстве выходы системы так же сложно, как и входы. Каждый сотрудник, например, в меру своей ответственности обязан заниматься задачами защиты информации и принимать меры по обеспечению ее безопасности. Меры по защите информации также включают разнообразные способы и средства, в том числе документы, определяющие доступ сотрудников к защищаемой информации в конкретном структурном подразделении организации.

Следовательно, **система защиты информации представляет собой модель системы, объединяющей силы и средства организации, обеспечивающие защиту информации**. Она описывается параметрами на рис. 1.1.

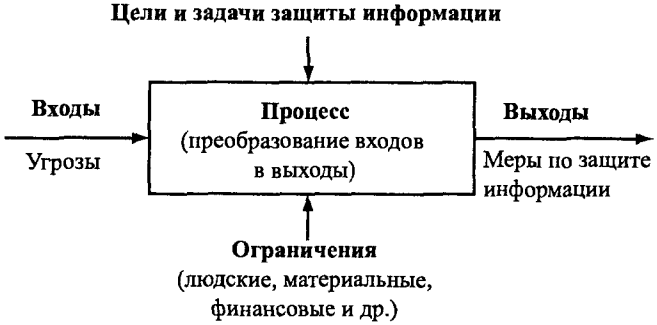



*Рис. 1.1.* Параметры системы защиты информации

К параметрам системы, по терминологии [2], относятся:

- цели и задачи (конкретизированные в пространстве и во времени цели);
- входы и выходы системы;
- ограничения, которые необходимо учитывать при построении (модернизации, оптимизации) системы;
- процессы внутри системы, обеспечивающие преобразование входов в выходы.

**Цели** представляют собой ожидаемые результаты функционирования системы защиты информации, а **задачи** то, что надо сделать для того, чтобы система могла обеспечить достижение поставленных целей. Возможность решения задач зависит от **ресурса**, выделяемого на защиту информации. Ресурс включает в себя людей, решающих задачи защиты информации, финансовые, технические и другие средства, расходуемые на защиту информации. **Входами** системы защиты информации являются угрозы информации, а **выходами** — меры, которые надо применить для предотвращения угроз или снизив их до допустимого уровня. Наконец, мероприятия, действия и технологии, определяющие меры защиты, соответствующие угрозам, образуют **процесс**.

Так как для слабоформализуемых задач нет методов их точного решения, то процесс представляет собой выбор для угроз на

**входе** системы рациональных вариантов защиты, удовлетворяющих значениям используемых показателей эффективности защиты. Следовательно, процесс выбора должен включать также **показатели эффективности**, по которым производится выбор мер из множества известных. При отсутствии формальных методов решения слабоформализуемых задач в общем случае можно обеспечить лишь выбор рациональных решений, удовлетворяющих определенным требованиям и образующих область решений, внутри которой находится оптимальное решение.

Решение проблемы защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы, не обеспечивающей требуемый уровень защищенности, в систему с заданным уровнем безопасности информации.

## 1.2. Цели, задачи и ресурсы системы защиты информации

Формулирование целей и задач защиты информации, как любой другой деятельности, представляет начальный и значимый этап обеспечения безопасности информации. Важность этого этапа часто недооценивается и ограничивается целями и задачами, напоминающими лозунги. В то же время специалисты в области системного анализа считают, что от четкости и конкретности целей и постановок задач во многом зависит успех в их достижении и решении. Провал многих, в принципе полезных, начинаний обусловлен именно неопределенностью и расплывчатостью целей и задач, из которых не ясно, кто, что и за счет какого ресурса предполагает решать продекларированные задачи.

Цели защиты информации сформулированы в ст. 20 Закона РФ «Об информации, информатизации и защите информации»:

- предотвращение утечки, хищения, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в ин-

формационные ресурсы и информационные системы, обеспечение правового режима как объекта собственности;
- защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

В общем виде цель защиты информации определяется как обеспечение безопасности информации, содержащей государственную или иные тайны. Но такая постановка цели содержит неопределенные понятия: **информация** и **безопасность**.

Информация — первичное понятие, используемое в понятийном аппарате информационной безопасности. Предпринимаются многочисленные попытки дать корректное определение понятию «информация», но список попыток пока не закрыт. Учитывая, что любой материальный объект или физическое явление отображаются в виде совокупности признаков (свойств), а человек, кроме того, на основе этих признаков формирует их модели или образы, то информацию можно представить как отображение реального или виртуального мира на языке признаков материальных объектов или абстрактных символов. Более подробно понятие «информация» рассмотрено в разд. II.

Основной целью защиты информации является обеспечение заданного уровня ее безопасности. Под заданным уровнем **безопасности информации** понимается такое состояние защищенности информации от угроз, при котором обеспечивается допустимый риск ее уничтожения, изменения и хищения. При этом под уничтожением информации понимается не только ее физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забытия пароля компьютера, искажения кода загрузочного сектора винчестера или дискетки и других факторах информация не искажается и не похи-

щается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создает. Однако при невозможности доступа к ней в нужный момент ее пользователь теряет информацию так же, как если бы она была уничтожена.

Угроза может быть реализована с различной вероятностью. Вероятность реализации угрозы безопасности информации определяет **риск** ее владельца. Допустимость риска означает, что ущерб в результате реализации угроз не приведет к серьезным последствиям для собственника информации. Ущерб может проявляться в разнообразных формах: неполучение прибыли, ожидаемой от информации при ее материализации в новой продукции или принятии более обоснованного решения; дополнительные затраты на замену образцов военной техники, характеристики которой стали известны вероятному противнику; и другие. По некоторым оценкам, например, попадание к конкуренту около 20% объема конфиденциальной информации фирмы может привести к ее банкротству.

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы. Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатационных и др. расходов. Наиболее общей формой представления ресурса является денежная мера. Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер. Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники, постоянный — на заработную плату сотрудникам службы безопасности и поддержание определенного уровня безопасности, прежде всего, путем эксплуатации технических средств и контроля эффективности защиты. Средний ресурс оценивается величиной денежных средств, выделяемых или расходуемых в среднем в год, как отношение расходов за определенный период на длительность этого периода в годах. При построении или модернизации системы защиты необходимые большие разовые расходы на созда-

ние или закупку технических средств защиты за достаточно большое время их применения (5–10 лет) окупаются.

Чем больше ресурс на защиту информации, тем более высокий уровень безопасности информации может он обеспечить. В принципе, при неограниченном ресурсе можно получить сколь угодно малую вероятность реализации угрозы. Если обозначить через $С_и$ и $Р_у$ цену информации и вероятность реализации угрозы соответственно, то ущерб от реализации угрозы можно оценить величиной $С_у = С_и Р_у$. Величину ущерба можно рассматривать как возможные (потенциальные) косвенные расходы, а ресурс — как прямые (учитываемые бухгалтерией) расходы $С_{пр}$ на защиту информации. Следовательно, владелец (пользователь) информации объективно вынужден нести расходы на нее, равные сумме прямых и косвенных расходов: $С_{ри} = С_{пр} + С_{кр}$. Между этими слагаемыми существует тесная связь — косвенные расходы обратно пропорциональны прямым расходам. Эта связь позволяет оценить на качественном уровне зависимость суммарных расходов на информацию от прямых расходов, качественно отображенной на рис. 1.2.

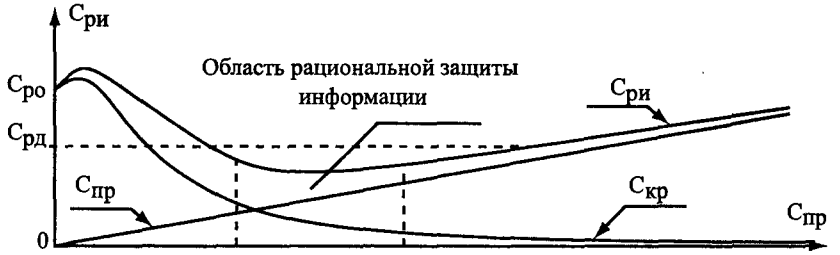



*Рис. 1.2.* Зависимость суммарных расходов на информацию от прямых расходов

Рост суммарных расходов на информацию при малых прямых расходах вызван тем обстоятельством, что эффект защиты начинает проявляться, когда прямые расходы превышают некоторую критическую массу. Например, для получения эффекта от средства защиты необходимо предварительно вложить средства в его покупку и установку.

Из этого рисунка следует, что при некоторых прямых расходах наблюдается область с минимальными суммарными расходами на

информацию. Эта область является **областью рациональной защиты информации**.

Задачи инженерно-технической защиты, как любые иные задачи, — не микроцели, как часто их определяют, а четкое и конкретное описание того, что надо сделать для достижения цели. Сформулировать задачи можно только тогда, когда определена защищаемая информация и угрозы ей. В постановке задачи указывается необходимость определения рациональных мер для конкретной защищаемой информации и угрозы ей с учетом имеющегося ресурса.

## 1.3. Угрозы безопасности информации и меры по их предотвращению

Угрозы безопасности информации — состояния и действия субъектов и материальных объектов, которые могут привести к изменению, уничтожению и хищению информации.

К угрозам безопасности информации относят также блокирование доступа к ней. Недоступность информации для ее законного владельца или пользователя в моменты времени, когда в ней возникает необходимость, по последствиям равносильна ее уничтожению. Любой активный пользователь компьютерной техники хоть раз испытал крайне неприятное состояние, когда из-за ошибки в загрузочном секторе жесткого диска становится недоступной информация, накапливаемая в течение длительного времени. Хотя с самой информацией ничего не произошло и в принципе через некоторое время можно восстановить доступ к ней (даже есть организации, зарабатывающие на этом деньги), эта угроза блокирования информации достаточно серьезная, так как ее реализация может привести к большому ущербу для владельца (пользователя). Например, несвоевременная отправка документа из-за блокирования его в компьютере или неисправности электронного замка сейфа может привести к нарушению контракта со всеми вытекающими из этого последствиями.

Угроза как потенциальная опасность для информации может быть реализована или нет. Но потенциальная опасность существует всегда, меняется только ее уровень. Количество потенциальных

угроз информации огромно: от очевидных прямых до неочевидных косвенных. Например, конфликт между администрацией организации и работником создает угрозу безопасности информации, так как недовольный сотрудник может в качестве орудия мести избрать секретную или конфиденциальную информацию. Угрозы создаются преднамеренно или возникают случайно как сопутствующие работе организации и ее сотрудников.

Следует отличать угрозы от результатов их реализации. Изменение, уничтожение, хищение и блокирование информации — это результаты реализации угроз или свершившиеся угрозы.

Наибольшую угрозу для информации, содержащей государственную тайну, создает зарубежная разведка. Основной интерес для нее представляют сведения в военной области, в области экономики, науки и техники, во внешней политике, в области разведывательной, контрразведывательной и оперативно-розыскной деятельности зарубежных государств, прежде всего, потенциальных противников и конкурентов, в том числе:

- о состоянии и прогнозах развития военного, научно-технического и экономического потенциалов государств;
- о достижениях науки и техники, содержании научно-исследовательских, опытно-конструкторских, проектных работ и технологий, имеющих важное оборонное и экономическое значение;
- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и боевой техники;
- о дислокации, составе, вооружении войск и состоянии их боевого обеспечения;
- об объемах запасов, добычи, поставки и потребления стратегических видов сырья, материалов и полезных ископаемых;
- о выполнении условий международных договоров, прежде всего, об ограничении вооружений и др.

Кроме этих глобальных вопросов органы зарубежной разведки добывают большой объем разнообразной информации, вплоть до состояния здоровья, характера, привычек, стиля мышления политических и военных руководителей зарубежных государств.

Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности на рынке в условиях острой конкурентной борьбы.

Задачи органов коммерческой разведки, их состав и возможности зависят от назначения и капитала фирмы, но принципы добывания информации существенно не отличаются. Основными предметными областями, представляющими интерес для коммерческой разведки, являются:

- коммерческая философия и деловая стратегия руководителей фирм-конкурентов, их личные и деловые качества;
- научно-исследовательские и конструкторские работы;
- финансовые операции фирм;
- организация производства, в том числе данные о вводе в строй новых, расширении и модернизации существующих производственных мощностей, объединение с другими фирмами;
- технологические процессы при производстве новой продукции, результаты ее испытаний;
- маркетинг фирмы, в том числе режимы поставок, сведения о заказчиках и заключаемых сделках, показатели реализации продукции.

Кроме того, коммерческая разведка занимается:

- изучением и выявлением организаций, потенциально являющихся союзниками или конкурентами;
  добыванием, сбором и обработкой сведений о деятельности потенциальных и реальных конкурентов;
  учетом и анализом попыток несанкционированного получения коммерческих секретов конкурентами;
- оценкой реальных отношений между сотрудничающими и конкурирующими организациями;
- анализом возможных каналов утечки конфиденциальной информации.

Сбор и анализ данных производится также по множеству других вопросов, в том числе изучаются с целью последующей вербовки сотрудники фирм-конкурентов, их потребности и финансовое положение, склонности и слабости.

Коммерческая разведка осуществляется методами **промышленного шпионажа** и **бизнес-разведки** (деловой, конкурентной, экономической разведки). Если основной целью промышленного шпионажа является добывание данных о разрабатываемой продукции, то основное направление бизнес-разведки — получение ин-

формации для руководства, необходимой для принятия им обоснованных управленческих решений. К этой информации относятся сведения о глобальных процессах в экономике, политике, технологии производства, партнерах и конкурентах, тенденциях рынка и других вопросах. Например, даже при покупке дорогого товара важно иметь информацию о его производителе и продавце, так как качество товара часто зависит как от специализации и опыта его производителя, так и от солидности его продавца. Продавец, берегущий свою репутацию, избегает сотрудничества с сомнительными поставщиками товара.

За рубежом созданы различные органы конкурентной разведки. Например, в США общество профессионалов конкурентной работы (Society of Competitive Intelligence Proffessionals SCIP) насчитывает около 6 тысяч человек и имеет отделения во многих странах мира. В Японии разветвленная система конкурентной разведки включает в себя службы разведки крупных фирм и государственных организаций.

Основные проблемы конкурентной разведки вызваны не только и не столько недостоверностью и недостаточностью информации, что характерно для промышленного шпионажа, но и чрезмерно большим количеством противоречивых данных и сведений по ее тематике. Поисковая система в Интернете может по запросу выдать огромное число данных, среди которых полезная информация разбросана как вкрапления ценных минералов в пустой породе. Поэтому основу составляют процессы поиска информации в открытых источниках и ее анализ с целью получения необходимых сведений.

Знание конкретных угроз защищаемой информации создает возможность постановки задач по **определению рациональных мер защиты информации**, предотвращающих угрозы или снижающих до допустимых значений вероятность их реализации. Меры по защите информации с позиции системного подхода рассматриваются как результаты функционирования системы защиты. Они могут представлять собой конкретные действия персонала, предложения по приобретению и установке технических и программных средств, требования к сотрудникам, определенные в соответствующих правовых документах, и т. д. В принципе для предо-

твращения или, по крайней мере, существенного снижения уровня конкретной угрозы безопасности информации можно предложить несколько мер по ее защите. Однако их эффективность может существенно отличаться. Выбор любой меры защиты информации, так же как в иной любой сфере, производится по показателям оценки эффективности, которые учитывают степень выполнения задачи и затраты ресурса на ее решение. Многообразие угроз безопасности информации порождает многообразие мер ее защиты. Эффективность каждой меры защиты безопасности информации оценивается своими **локальными (частными) показателями эффективности**. Их можно разделить на **функциональные (оперативные)** и **экономические**. Функциональные показатели характеризуют уровень безопасности информации, экономические — расходы на ее обеспечение. Так как уровень безопасности информации определяется величиной потенциального ущерба от реализации угроз, то в качестве локальных функциональных показателей эффективности защиты информации используются как показатели количества и качества информации, которая может попасть к злоумышленнику, так и характеристики реально возникающих угроз безопасности информации.

Эффективность системы защиты информации в целом определяется глобальными функциональным и экономическим критериями или показателями. В качестве функционального глобального критерия часто используется «взвешенная» сумма функциональных локальных показателей. Если обозначить через $\omega_i$ значение i-го локального показателя, то глобальный показатель определяется как $W_г = \sum_{\forall i} \alpha_i \omega_i$, причем $\sum_{\forall i} \alpha_i = 1$. Коэффициент $\alpha_i$ характеризует «вес» локального показателя. Физического смысла такой показатель не имеет. Глобальный экономический показатель представляет собой меру суммарных расходов на информацию.

Эффективность тем выше, чем ниже расходы при одинаковом уровне безопасности информации или чем больше уровень ее безопасности при одинаковых расходах. Первый подход к оценке эффективности используется при отсутствии жестких ограничений на ресурс, выделяемый для защиты информации, второй — при заданном ресурсе.

## Вопросы для самопроверки

1. Почему для слабоформализуемых задач сложно найти оптимальное решение?
2. Чем отличается система от совокупности ее элементов?
3. Особенности системы инженерно-технической защиты по сравнению с системой в виде структурного подразделения, организации или учебного заведения.
4. Параметры системы защиты.
5. Что представляет собой процесс системы инженерно-технической защиты информации?
6. Особенности системного мышления.
7. Что надо априори знать для формулирования целей и задач инженерно-технической защиты информации?
8. Что представляет собой ресурс системы защиты информации?
9. Чему равны суммарные расходы на информацию?
10. Физический смысл рациональной области защиты информации.
11. Что надо определить перед выбором мер защиты информации?
12. Что представляют собой локальные и глобальный показатели эффективности защиты информации?

# Глава 2. Основные положения концепции инженерно-технической защиты информации

Основные положения концепции инженерно-технической защиты информации определяют ее принципы, которые конкретизируются в методах, способах и средствах инженерно-технической защиты информации. Если цель отвечает на вопрос, что надо достичь в результате инженерно-технической защиты информации, а задачи — что надо сделать для этого, то принципы дают общее представление о подходах к решению поставленных задач. Принципы можно разделить на принципы инженерно-технической защиты информации как процесса и принципы построения системы инженерно-технической защиты информации.

## 2.1. Принципы инженерно-технической защиты информации

Любая технология, в том числе защиты информации, должна соответствовать набору определенных общих требований, которые можно рассматривать как общие принципы защиты информации. К ним относятся:

- надежность защиты информации;
- непрерывность защиты информации;
- скрытность защиты информации;
- целеустремленность защиты информации;
- рациональность защиты;
- активность защиты информации;
- гибкость защиты информации;
- многообразие способов защиты;
- комплексное использование различных способов и средств защиты информации;
- экономичность защиты информации.

**Надежность защиты информации** предусматривает обеспечение требуемого уровня ее безопасности независимо от внешних и внутренних факторов, влияющих на безопасность информации. При рациональной защите на ее уровень не должны влиять как

преднамеренные действия злоумышленника, например выключение электропитания, так и стихийные силы, например пожар.

**Непрерывность защиты информации** характеризует постоянную готовность системы защиты к отражению угроз информации. Так как место и время угрозы информации априори неизвестны, то в инженерно-технической защите не может быть перерывов в работе, в том числе в ночное время.

Затраты на изменения системы защиты минимизируются в случае **скрытности защиты информации**. Чем выше скрытность, тем больше неопределенность исходных данных у злоумышленника и тем меньше у него возможностей по добыванию информации. Скрытность защиты информации достигается скрытным (тайным) проведением мер по защите информации и существенным ограничением допуска сотрудников организации (предприятия, учреждения) к информации о конкретных способах и средствах инженерно-технической защиты информации в организации.

Так как ресурса на нейтрализацию всех угроз, как правило, не хватает, **то целеустремленность защиты информации** предусматривает сосредоточение усилий по предотвращению угроз наиболее ценной информации.

В то же время инженерно-техническая защита информации должна быть **рациональной**, которая предполагает минимизацию ресурса, расходуемого на обеспечение необходимого уровня безопасности информации.

Недостоверность и недостаточность информации об угрозах информации может быть в какой-то степени компенсированы ее поиском. Поговорка «пока гром не грянет, мужик не перекрестится» не приемлема для обеспечения защиты информации. Необходимым условием эффективной защиты информации является ее **активность**, которая обеспечивается, прежде всего, прогнозированием угроз и созданием превентивных мер по их нейтрализации. Активность защиты соответствует активности обороны — одному из важнейших принципов ведения оборонительных войсковых операций. Опыт их ведения позволяет утверждать, что даже очень мощная, но пассивная оборона в конце концов может быть разрушена и завершиться поражением. Только постоянные контратаки, не дающие противнику возможность хорошо подготовиться к наступлению, могут привести к победе в обороне.

Добывание и защита информации — это процесс борьбы противоположных сил. Учитывая, что основным источником угроз является человек — злоумышленник, победа в ней возможна при **гибкости защиты информации**. Необходимость ее обусловлена, прежде всего, свойством информации к растеканию в пространстве. Со временем все больше деталей системы защиты становятся известны большему числу сотрудников и, следовательно, будут более доступными и злоумышленнику. Гибкость защиты предполагает возможность оперативно изменять меры защиты, особенно в случае, если принимаемые меры станут известны злоумышленнику. Гибкость защиты информации можно обеспечить, если система имеет набор разнообразных мер защиты, из которого можно оперативно выбрать эффективные для конкретных угроз и условий. Гибкость обеспечивается **многообразием способов и средств** инженерно-технической защиты информации.

Так как нет универсальных методов и средств защиты информации, то существует необходимость в их таком **комплексном применении**, при котором недостатки одних компенсируются достоинствами других.

Наконец, защита информации должна быть **экономичной**. Это значит, что затраты на защиту информации не должны превышать возможный ущерб от реализации угроз.

Рассмотренные общие принципы инженерно-технической защиты информации не дают конкретных рекомендаций по инженерно-технической защите информации. Однако они ориентируют специалиста на требования, которым должна соответствовать инженерно-техническая защита информации.

## 2.2. Принципы построения системы инженерно-технической защиты информации

При разработке принципов построения системы инженерно-технической защиты информации учитывались рассмотренные принципы, принципы обеспечения безопасности живых существ, используемых природой, и известные пути нейтрализации различных угроз человеком.

Так как информационная безопасность является частью предметной области, определяемой общим понятием «безопасность»,

включающей и безопасность живых существ, то полезную подсказку по мерам обеспечения информационной безопасности можно получить в результате анализа решений этой проблемы природой. Проблема безопасности в живой природе крайне важна, так как от эффективности ее решения зависит сохранение видов живых существ. Способы защиты в живой природе доказали свою эффективность за длительный период эволюции и могут быть полезными для обеспечения информационной безопасности. Они рассмотрены С. П. Расторгуевым в [3] и приведены на рис. 2.1.

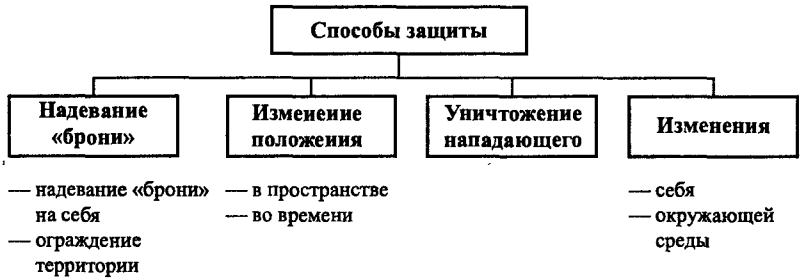



*Рис. 2.1.* Природные способы защиты живых существ

Для защиты от хищников некоторые живые существа создают механические преграды («броню»), которые надевают на себя (черепахи, ежи, раки и др.), или в виде своего «дома» (пчелы, осы, норковые животные и др.). Другие, не имеющие такой «брони», имеют длинные ноги, развитые крылья или плавники и спасаются от врага бегством (изменением местоположения) или обеспечивают сохранение вида интенсивным размножением. Например, многие насекомые и даже растения выживают благодаря своей плодовитости, которая компенсирует массовую гибель беззащитных особей. Третья группа живых существ снабжена мощными клыками, когтями, рогами и другими средствами защиты, способными отогнать или уничтожить нападающего. Наконец, четвертая группа, не имеющая указанных средств защиты, выживает путем маскировки себя (мимикрии) под окружающую среду, изменения характеристик окружающей среды с целью дезориентации хищника (хамелеон, осьминог и др.), а также миметизма (отпугивания грозным внешним видом). Например, бабочка «вицерой» принимает окраску

ядовитой бабочки «монарх», безвредная «змеиная» гусеница имитирует движение змеи и т. д.

Против угроз воздействий различных сил человечество за свою историю выработало достаточно эффективные меры в виде различных естественных и искусственных рубежей защиты. В средние века человек надевал на себя металлические или кожаные доспехи (сейчас — бронежилеты), окружал дома и города высокими и мощными стенами и заборами, что продолжает делать и сейчас. Наиболее распространенный способ защиты преступников от органов правосудия — убегание. Наконец, возможности человека по изменению своего внешнего вида или окружающей среды существенно превосходят все то, на что способна «неразумная» природа.

Учитывая, что **угрозы воздействия на информацию** представляют собой силы различной физической природы (механической, электрической, электромагнитной, тепловой и др.), система защиты должна создавать вокруг носителей информации с локальными размерами преграды — рубежи защиты от этих сил.

В отличие от сил воздействий, направленных на источники информации, **утечка информации** происходит при распространении носителей с защищаемой информацией от ее источников. Мерами защиты от утечки являются также преграды, создаваемые вокруг источников информации. Но эти преграды должны задержать не силы воздействий, а носителей информации.

На источник информации как объект защиты могут быть распространены принципы и способы защиты, используемые природой и созданные человеком, в том числе подходы к созданию абсолютной системы защиты, рассмотренные в [3]. Под **абсолютной системой** понимается система, обеспечивающая полную (гарантированную) защиту при любых угрозах. Абсолютная система определена как система, обладающая всеми возможными способами защиты и способная в любой момент своего существования спрогнозировать наступление угрожающего события за время, достаточное для приведения в действия адекватных мер по нейтрализации угроз.

Абсолютная система является гипотетической, идеальной, так как любая реальная система защиты не может в принципе обладать

всеми характеристиками и свойствами абсолютной. Механизмы прогнозирования и принятия решений в процессе функционировании допускают ошибки. Кроме того, следует иметь в виду, что органы разведки и подготовленные злоумышленники хорошо осведомлены о современных способах защиты и активны в поиске нетиповых вариантов обмана механизма прогнозирования и обхода мер защиты. Однако реализация механизмов абсолютной системы в реальной системе позволит приблизиться к возможностям идеальной защиты.

Следовательно, система защиты информации должны содержать:

- рубежи вокруг источников информации, преграждающих распространение сил воздействия к источникам информации и ее носителей от источников;
- силы и средства достоверного прогнозирования и обнаружения угроз;
- механизм принятия решения о мерах по предотвращению или нейтрализации угроз;
- силы и средства нейтрализации угроз, преодолевших рубежи защиты.

Основу построения такой системы составляют следующие принципы:

- многозональность пространства, контролируемого системой инженерно-технической защиты информации;
- многорубежность системы инженерно-технической защиты информации;
- равнопрочность рубежа контролируемой зоны;
- надежность технических средств системы защиты информации;
- ограниченный контролируемый доступ к элементам системы защиты информации;
- адаптируемость (приспособляемость) системы к новым угрозам;
- согласованность системы защиты информации с другими системами организации.

**Многозональность защиты** предусматривает разделение (территории государства, организации, здания) на отдельные контролируемые зоны, в каждой из которых обеспечивается уровень безопасности, соответствующий цене находящейся там информации. На территории Советского Союза создавались зоны, закрытые для иностранцев, приграничные зоны, закрытые города. Уровень безопасности в любой зоне должен соответствовать максимальной цене находящейся в ней информации. Если в ней одновременно размещены источники информации с меньшей ценой, то для этой информации уровень безопасности, а следовательно, затраты будут избыточными. Так как уровень безопасности в каждой зоне определяется исходя из цены находящейся в ней информации, то многозональность позволяет уменьшить расходы на инженерно-техническую защиту информации. Чем больше зон, тем более рационально используется ресурс системы, но при этом усложняется организация защиты информации. Зоны могут быть **независимыми, пересекающимися и вложенными** (рис. 2.2).

Для **независимых зон** уровень безопасности информации в одной зоне не зависит от уровня безопасности в другой. Они создаются для разделения зданий и помещений, в которых выполняются существенно отличающиеся по содержанию и доступу работы. Например, администрация организации размещается в одном здании, научно-исследовательские лаборатории — в другом, а производственные подразделения — в третьем.

Примером **пересекающихся зон** является приемная руководителя организации, которая, с одной стороны, принадлежит зоне с повышенными требованиями к безопасности информации, источниками которой являются руководящий состав организации и соответствующие документы в кабинете, а с другой стороны, в приемную имеют доступ все сотрудники и посетители организации. Требования к безопасности информации в пересекающейся зоне являются промежуточными между требованиями к безопасности в пересекающихся зонах. Например, уровень безопасности в приемной должен быть выше, чем в коридоре, но его нельзя практически обеспечить на уровне безопасности информации в кабинете.

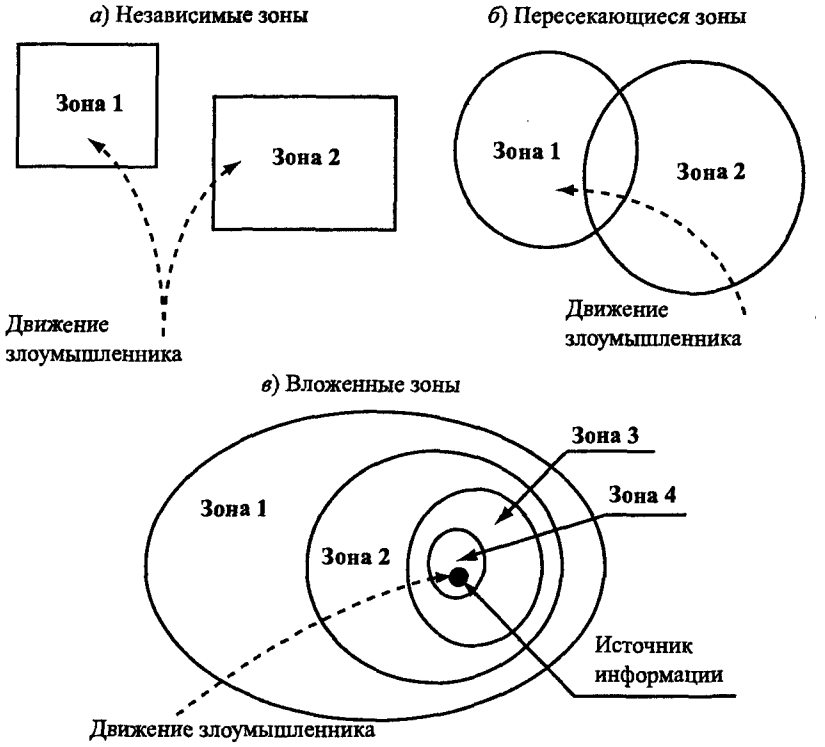



*Рис. 2.2.* Виды конролируемых зон

**Вложенные зоны** наиболее распространены, так как позволяют экономнее обеспечивать требуемый уровень безопасности информации. Безопасность информации i-й вложенной зоны определяется не только ее уровнем защиты, но и уровнями защиты в предшествующих зонах, которые должен преодолеть злоумышленник для проникновения в i-ю зону.

Каждая зона характеризуется уровнем безопасности находящейся в ней информации. Безопасность информации в зоне зависит от:

- расстояния от источника информации (сигнала) до злоумышленника или его средства добывания информации;
- количества и уровня защиты рубежей на пути движения злоумышленника или распространения иного носителя информации (например, поля);

- эффективности способов и средств управления допуском людей и автотранспорта в зону;
- мер по защите информации внутри зоны.

Чем больше удаленность источника информации от места нахождения злоумышленника или его средства добывания и чем больше рубежей защиты, тем большее время движения злоумышленника к источнику и ослабление энергии носителя в виде поля или электрического тока. Количество и пространственное расположение зон и рубежей выбираются таким образом, чтобы обеспечить требуемый уровень безопасности защищаемой информации как от внешних (находящихся вне территории организации), так и внутренних (проникших на территорию злоумышленников и сотрудников). Чем более ценной является защищаемая информация, тем большим количеством рубежей и зон целесообразно окружать ее источник и тем сложнее злоумышленнику обеспечить разведывательный контакт с ее носителями. Вариант классификация зон по условиям доступа приведен в табл. 2.1 [4].

*Таблица 2.1*

| *Категория зоны* | *Наименование зоны* | *Функциональное назначение зоны* | *Условия доступа сотрудников* | *Условия доступа посетителей* |
|---|---|---|---|---|
| 0 | Свободная | Места свободного посещения | Свободный | Свободный |
| I | Наблюдаемая | Комнаты приема посетителей | Свободный | Свободный |
| II | Регистрационная | Кабинеты сотрудников | Свободный | По удостоверению личности с регистрацией |
| III | Режимная | Секретариат, компьютерные залы, архивы | По идентификационным картам | По разовым пропускам |
| IV | Усиленной защиты | Кассовые операционные залы, материальные склады | По спецдокументам | По спецпропускам |
| V | Высшей защиты | Кабинеты высших руководителей, комнаты для ведения переговоров, специальные хранилища | По спецдокументам | По спецпропускам |

Из анализа этой таблицы следует, что по мере увеличения категории зоны усложняются условия допуска как сотрудников, так и посетителей.

На границах зон и особо опасных направлений создаются **рубежи защиты**. Очевидно, что чем больше рубежей защиты и чем они надежнее (прочнее), чем больше времени и ресурса надо потратить злоумышленнику или стихийным силам на их преодоления. Рубежи защиты создаются и внутри зоны на пути возможного движения злоумышленника или распространения иных носителей, прежде всего, электромагнитных и акустических полей. Например, для защиты акустической информации от подслушивания в помещении может быть установлен рубеж защиты в виде акустического экрана.

Типовыми зонами организации, указанными на рис. 2.3, являются:

- территория, занимаемая организацией и ограничиваемая забором или условной внешней границей;
- здание на территории;
- коридор или его часть;
- помещение (служебное, кабинет, комната, зал, техническое помещение, склад и др.);

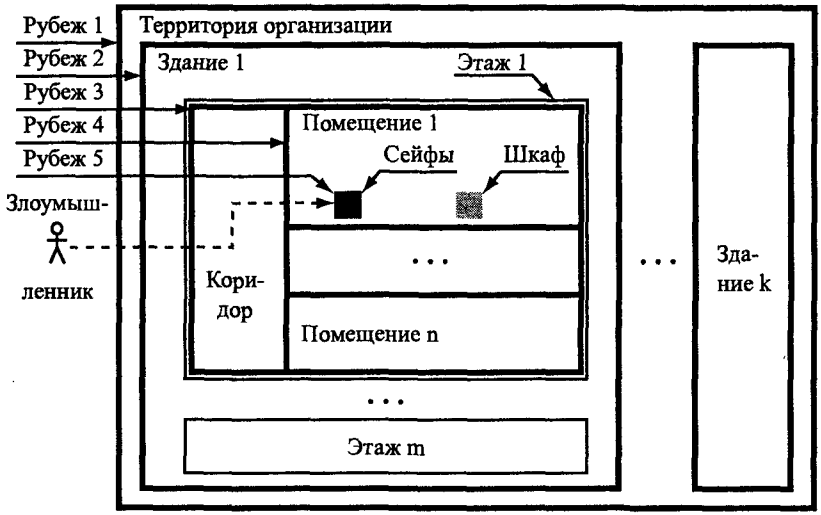



*Рис. 2.3.* Типовые зоны и рубежи организации

- шкаф, сейф, хранилище.

Соответственно, рубежи защиты:

- забор;
- стены, двери, окна здания;
- двери, окна (если они имеются), стены, пол и потолок (перекрытия) коридора;
- двери, окна, стены, пол и потолок (перекрытия) помещения;
- стены и двери шкафов, сейфов, хранилищ.

Необходимым условием и принципом эффективной инженерно-технической защиты информации является **равнопрочность рубежа** контролируемой зоны. Наличие бреши в защите может свести на нет все затраты. В качестве классического примера последствий невыполнения этого требования можно привести линию Мажино, образованную накануне Второй мировой войны мощными французскими оборонительными укреплениями возле границ с Германией, которая, по мнению руководства Франции, должна была надежно защитить ее от агрессии. Но немцы без особенных усилий обошли эту линию через Бельгию и вошли в Париж. Выполнение принципа равнопрочности рубежа требует выявления и анализа всех потенциальных угроз с последующей нейтрализацией угроз с уровнем выше допустимого.

**Непрерывность защиты** информации может быть обеспечена при условии безотказной работы сил и средств системы защиты. **Надежность** любого **технического средства** всегда ниже 100%. Поэтому через некоторое время, усредненное значение которого называется временем безотказной работы, в нем возникает неисправность. Ущерб от неисправности технических средств защиты может быть очень высокий, равный цене информации. Если техническое средство охраны своевременно не среагирует на угрозу, например пожара в помещении ночью, то за время, когда его обнаружит дежурная смена в другом конце здания или посторонние лица за забором, могут сгореть все документы, находящиеся в этом помещении. Ложные срабатывания средств защиты при отсутствии угроз менее опасны, но они способствуют формированию у охраны психологической установки на то, что причиной срабатывания средства защиты является его неисправность. Такая установка увеличивает время реакции сотрудника охраны на угрозу.

Этим пользуются иногда преступники, которые перед проникновением в контролируемую зону вызывают многократные срабатывания средств защиты, в результате которых сотрудники охраны перестают на них реагировать. Поэтому к надежности технических средств защиты предъявляются повышенные, по сравнению с другими средствами, требования, а сами средства многократно дублируюся. Например, в помещении устанавливается, как правило, несколько датчиков (извещателей) пожарной сигнализации.

Необходимым условием обеспечения скрытности защиты информации является **жесткий контроль и управление допуском к элементам системы защиты**, в том числе к ее техническим средствам. Выполнение этого принципа построения системы защиты требует скрытности и дополнительной укрепленности мест размещения технических средств защиты информации.

**Гибкость защиты** информации обеспечивается **адаптируемостью системы** к новым угрозам и изменением условий ее функционирования. Для оперативной адаптации необходимы механизмы быстрого изменения структуры системы и резерв ее сил и средств.

Система защиты информации функционирует совместно с другими системами государства и организации любого уровня. Поэтому она должна функционировать **согласованно с другими системами**. В противном случае эти системы будут мешать друг другу. Можно в интересах инженерно-технической защиты информации настолько ужесточить режим безопасности в организации, что ее сотрудникам будет сложно выполнять свою основную работу. Например, в некоторых режимных организациях разрешают размножать (печатать) закрытые документы только в машинописном бюро, небольшое количество сотрудников-машинисток которого не справляется с работой в конце года, когда резко возрастает число отчетных документов. В результате этого организацию периодически лихорадит. Следовательно, необходимы иные решения по обеспечению безопасности информации, существенно не затрудняющие работу организации по иным видам деятельности. Конечно, меры по защите информации в той или иной степени ужесточают режим организации, но чем незаметнее система защиты информации решает свои задачи, тем более она рациональ-

на. Следовательно, рационально построенная система инженерно-технической защиты информации должна минимизировать дополнительные задачи и требования, вызванные мерами по защите информации, к сотрудникам организации.

Чем более универсальной является любая система, тем она менее эффективно решает конкретные задачи по сравнению с узко специализированной системой. «Плату» за универсальность можно снизить введением в систему механизма адаптации ее конфигурации и алгоритма функционирования ее к изменившимся условиям. Этот принцип широко используется в современном строительстве: сигнальные (для передачи информационных сигналов) кабели и кабели электропитания размещаются не в железобетонных стенах, а в предусмотренном проектами пространстве с легким доступом между межэтажными перекрытиями и потолком или полом. Конечно, в этом случае несколько ухудшается пожароустойчивость помещения, но обеспечивается возможность экономичного и быстрого изменения схемы коммуникаций.

**Адаптируемость** системы защиты информации достигается прогнозированием угроз и заложенной при ее создании возможности производить без капитальных вложений изменения элементов как физической защиты, так и скрытия источников информации.

Кроме защиты информации в любой организации решается множество других задач по безопасности сотрудников не только на рабочем месте, но и в иных местах, по защите материальных ценностей, размещенных в разных местах ее территории (во дворе, на складах, в помещениях и др.). Поэтому наряду с системой защиты информации в организации создаются и иные системы. Автономное их функционирование распыляет средства, что в условиях их ограниченности снижает эффективность любой из этих систем.

### Вопросы для самопроверки

1. Принципы обеспечения инженерно-технической защиты информации.
2. Почему защита информации должна проводиться скрытно?
3. Что значит экономичность защиты информации?

4. Природные способы защиты живых существ.
5. Какие механизмы должна иметь абсолютная система защиты?
6. Принципы построения системы инженерно-технической защиты информации.
7. Сущность принципа адаптируемости системы защиты информации.
8. Что обеспечивает многозональность защиты информации?
9. Преимущества вложенных зон защиты информации.
10. Типовые контролируемые зоны организации.
11. Назначение рубежей защиты информации.
12. Типовые рубежи инженерно-технической защиты информации.

**Основные положения раздела I**

1. Инженерно-техническая защита информации является одним из основных направлений обеспечения информационной безопасности. Технический прогресс способствует повышению роли инженерно-технической защиты. Она охватывает большое количество областей знаний и сфер практической деятельности, при ее обеспечении необходимо учитывать большое число факторов, информация о которых недостаточная и часто недостоверная. Определяющую роль при инженерно-технической защите играет человек, действия которого пока не поддаются формализации. Задачи инженерно-технической защиты информации относятся к так называемым слабоформализуемым задачам, не имеющим формальных (строго математических) методов решения. Получение рациональных (удовлетворяющих поставленным требованиям) результатов при решении слабоформализуемых задач достигается на основе системного подхода.

2. Системный подход представляет собой обобщение опыта человечества по решению задач, прежде всего, слабоформализуемых. Эти задачи характеризуются большим числом факторов, влияющих на результат решения задачи, информация о которых недостоверная и недостаточная, и отсутствием формальных методов решения, учитывающих эти факторы. Отсутствие формального математического аппарата оптимизации решения слабоформализуемых задач не позволяет находить оптимальные решения. Результаты решения, удовлетворяющие требованиям, образуют

область рациональных решений, внутри которых находится оптимальный результат.

Системный подход предусматривает представление совокупности сил, средств и методов, обеспечивающих решение задач, в виде открытой системы, являющейся подсистемой более сложной системы и одновременно гиперсистемой для систем (подсистем) более низкого уровня. Система защиты не имеет юридически оформленной организационно-штатной структуры, а является моделью для анализа и разработки эффективной инженерно-технической защиты информации. Система защиты информации описывается пятью параметрами: целью и задачами защиты информации, ресурсами, угрозами — входами, мерами по защите информации — выходами и процессом преобразования входов в выходы. Системный подход требует полноты и достоверности описания параметров, в противном случае возможны грубые ошибки. Кроме того, при анализе системы надо учитывать появление в системе системных свойств, отсутствующих у ее элементов. Задачи защиты информации, как любые иные слабоформализуемые задачи, решаются путем выбора специалистом рациональных вариантов решения на основе результатов системного анализа. Основным аппаратом системного анализа является аппарат исследования операций — совокупность математических методов оптимизации решений сложных задач: теории массового обслуживания, линейного, нелинейного, динамического программирования, игр и др. Рациональный вариант выбирается по значениям показателей эффективности защиты информации. В зависимости от вида защищаемой информации и условий обеспечения безопасности информации применяются соответствующие показатели эффективности.

3. Основной целью инженерно-технической защиты информации является обеспечение ее безопасности, при которой риск изменения, уничтожения или хищения информации не превышает допустимого значения. Риск характеризуется вероятностью реализации угроз и зависит от ресурса — прямых расходов на защиту информации. Сумма прямых расходов на защиту информации и косвенных расходов, соответствующих ущербу от реализации угроз, определяет расходы на информацию. Значения прямых расходов, при которых суммарные расходы на информацию минимизиру-

ются, образуют область рациональной защиты информации. Для оценки риска необходимо определить источники информации и цену содержащейся в них информации, угрозы ее безопасности и возможность (вероятность) их реализации.

Задачи инженерно-технической защиты информации определяют то, что надо выполнить с учетом данного ресурса для предотвращения (нейтрализации) конкретных угроз в интересах поставленных целей.

4. Входы системы представляют собой угрозы безопасности информации. Угрозы проявляются в виде угроз преднамеренных и случайных (непреднамеренных) воздействий на источники информации и угроз утечки информации. Угрозы воздействий создают условия и действия, которые могут привести к непосредственному или дистанционному контакту сил человека и природы с источником информации, в результате которого информация может быть изменена, уничтожена, похищена или блокирована. Случайные воздействия в отличие от преднамеренных возникают в результате непреднамеренных (случайных) воздействий на источники информации людей, технических средств и стихийных сил.

5. Выходы системы защиты информации — меры по обеспечению инженерно-технической защиты. Меры инженерно-технической защиты информации представляют собой совокупность технических средств и способов их использования, которые обеспечивают требуемый уровень безопасности информации при минимуме ресурса. Каждому набору угроз соответствует рациональный набор мер защиты. Определение такого набора является основной задачей инженерно-технической защиты информации. При отсутствии формальных методов определение набора средств задача решается путем выбора этих мер специалистами по локальным и глобальным показателям эффективности.

6. Основу концепции инженерно-технической защиты информации составляют принципы ее защиты и построения системы инженерно-технической защиты информации.

Основными принципами инженерно-технической защиты информации являются:

- надежность, предусматривающая обеспечение требуемого уровня безопасности защищаемой информации;
- непрерывность защиты во времени и пространстве, характеризующая постоянную (в любое время) готовность системы защиты к предотвращению (нейтрализации) угроз информации;
- активность, предусматривающая упреждающее предотвращение (нейтрализация) угроз;
- скрытность, исключающая возможность ознакомления лиц с информацией о конкретных способах и средствах защиты в рассматриваемой структуре в объеме, превышающем служебную необходимость;
- целеустремленность, предполагающая расходование ресурса на предотвращение угроз с максимальным потенциальным ущербом;
- рациональность, требующая минимизации расходования ресурса на обеспечение необходимого уровня безопасности информации;
- комплексное использование различных способов и средств защиты информации, позволяющее компенсировать недостатки одних способов и средств достоинствами других;
- экономичность защиты, предусматривающая, что расходы на защиту не превысят ущерба от реализации угроз.

7. Принципы построения системы защиты информации учитывают рассмотренные принципы, способы безопасности живых существ, отобранные природой в процессе ее эволюции, способы, которые создали люди и механизмы гипотетической абсолютной системы обеспечения безопасности. К основным принципам построения инженерно-технической защиты информации относятся:

- многозональность пространства, контролируемого системой инженерно-технической защиты информации, позволяющая обеспечить согласование затрат на защиту и цены информации;
- многорубежность системы инженерно-технической защиты информации, увеличивающей время движения источников угроз и уменьшающей энергию сил воздействия и носителей информации при ее утечке;

- равнопрочность рубежей контролируемой зоны, исключающая появление в них «дырок», через которые возможно проникновение источников угроз и утечки информации;
- надежность технических средств системы защиты, обеспечивающая их постоянную работоспособность;
- ограниченный контролируемый доступ к элементам системы защиты информации, исключающий «растекание» информации о способах и средствах защиты;
- адаптируемость (приспосабливаемость) системы к новым угрозам и изменениям условий ее функционирования;
- согласованность системы защиты информации с другими системами, минимизирующая дополнительные задачи и требования к сотрудникам организации, вызванные необходимостью защиты информации.

## Литература к разделу I


1. *Ожегов С. И.* Словарь русского языка. — М.: Советская энциклопедия, 1968.
2. *Оптнер С. Л.* Системный анализ для решения деловых и промышленных проблем. — М.: Советское радио, 1969.
3. *Расторгуев С. П.* Абсолютная система защиты // Системы безопасности, связи и телекоммуникаций. — 1996. — Июнь–июль.
4. *Поздняков Е. Н.* Защита объектов (Рекомендации для руководителей и сотрудников служб безопасности). — М.: Банковский Деловой Центр, 1997.

# Раздел II. Теоретические основы инженерно-технической защиты информации

Теоретические основы инженерно-технической защиты информации конкретизируют положения концепции и представляют собой совокупность взаимоувязанных моделей объектов защиты, угроз информации и мер по их предотвращению или хотя бы снижению.

Любая модель является описанием элементов реального мира на языке моделирования. Модель, описывающая их на языке национального общения, называется описательной или вербальной. Так как язык национального общения допускает множество толкований, то вербальные модели неоднозначные. Поэтому наука стремится к наиболее полному и точному описанию мира, создавая формальные модели. Так как наиболее точной областью науки является математика, то основу любой полноценной теории составляют модели на языке математики. Однако если описываемые процессы сложны, недостаточно изучены и не поддаются формализации, то теория представляет собой совокупность вербальных моделей с элементами формальных моделей. К таким моделям относится теория инженерно-технической защиты информации.

## Глава 3. Характеристика защищаемой информации

### 3.1. Понятие о защищаемой информации

Первым вопросом, на которые должна ответить теория инженерно-технической защиты информации, — что представляет собой защищаемая информация?

Хотя существует множество определений информации, понятие «информация» не имеет пока строго научного однозначного определения и имеет в разных сферах деятельности различное смысловое наполнение. Например, в [28] приведены 28 вариантов определения понятия «информация».

В соответствии с терминологией Закона «Об информации, информатизации и защите информации» информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1]. По С. И. Ожегову, сведения — это знания [2]. Следовательно, информацию также можно рассматривать как знания в самом широком значении этого слова. Не только образовательные или научные знания, а любые сведения и данные, которые присутствуют в любом объекте и необходимы для функционирования любых информационных систем (живых существ или созданных человеком).

Однако такое представление об информации крайне расплывчатое. Более конкретное представление можно получить об информации в результате следующих рассуждений.

В общем случае любой материальный объект (физический процесс) обладает веществом и энергией, которыми он обменивается при взаимодействии с другими объектами. Энергия E и масса вещества m связаны известной зависимостью А. Эйнштейна $E = mc^2$. При взаимодействии объектов выполняются законы сохранения энергии и симметрии. Это значит, сколько один объект отдает энергии или вещества, столько другой объект их получает. Общий баланс энергии и вещества сохраняется при их взаимном переходе.

При обмене энергией и веществом происходит изменение признаков (значений характеристик) взаимодействующих объектов. При соударении биллиардных шаров движущийся шар отдает неподвижному не только свою кинетическую энергию, он изменяет его признаки или, другими словами, неподвижный шар получает информацию об энергии и свойствах движущегося.

Другой пример. Один человек сообщает другому, что книга с таким-то названием содержит много полезной информации. Однако после прочтения послушавший совета человек придерживается иного мнения. Следовательно, одна и та же книга при взаимодействии (чтении) ее с разными людьми по-разному изменяет их признаки. Один получает много полезной информации, другой нет. Это возможно только в том случае, если исходные априорные совокупности признаков двух человек отличаются на величину разности изменений их признаков после прочтения книги.

Признак объекта отображается в параметрах его вещества и полей. Любое внешнее воздействие вызывает изменения этих параметров. Например, камень скалы подвергается воздействию ультрафиолетовых и инфракрасных лучей Солнца, ветра, осадков, в результате чего изменяются его внешний вид, размеры, структура поверхности и другие признаки. Этот камень несет на себе признаки многовековых воздействий, признаки «веков».

Изменения значений признаков при взаимодействии неживых объектов случайные и приводят к увеличению их энтропии. При взаимодействии объектов, из которых хотя бы один относится к живой природе, эти изменения могут быть целенаправленными, уменьшающими энтропию живого существа.

Любой объект, процесс, явление могут быть описаны набором признаков. Количество признаков объектов в принципе может быть сколь угодно большим. Совокупность упорядоченных по времени n признаков, принадлежащих объекту, образует его **признаковую структуру** $П_{ст}$. Ее можно представить в виде объединения всех упорядоченных признаков объекта:

$$П_{ст}(t) = \bigcup_{i=1}^{n} П_i^j(t),$$

где $П_i^j(t)$ — j-е значение i-го признака в момент времени t.

В общем случае для описания объекта имеет значение не только количество и информативность признаков, но и последовательность и время их проявления. Последовательность проявления признаков объекта описывает на языке признаков его функционирование (деятельность). Например, технологические процессы производства продукции определяются не только набором операций, но и их последовательностью, а для химических технологий часто определяющим является и время выполнения технологической операции. Изменение признаков объекта целесообразно интерпретировать как получение им информации, приведшей к изменению этих признаков. Следовательно, под **полученной объектом информацией понимается разность между его признаковыми структурами после и до взаимодействия с другими объектами**. Соответственно, количество информации пропорционально величине этой разности.

Строго говоря, об информации можно корректно говорить во время и после взаимодействия объектов. До взаимодействия ничего определенного сказать об информации, содержащейся в признаках объектов, нельзя. Например, как можно оценить информацию в книге до ее прочтения? Можно только указать ее видовые и другие признаки, в том числе толстая книга или тонкая. Но признаки любого объекта содержат потенциальную информацию, которая становится реальной при взаимодействии его с другими. Так как окружающий мир состоит из материальных объектов, процессов и явлений, то совокупность их признаков образует пространство признаков или информационное поле, из которого любой объект может получить столько информации, сколько он способен воспринять. Следовательно, любой материальный объект может рассматриваться как носитель информации, которая приобретает конкретный вид и меру при взаимодействии его с другими объектами. Если представить признаковую структуру в виде области в n-мерном пространстве, каждая координата которого соответствует одному из признаков, то изменение признаков — получение информации одним объектом при взаимодействии с другим — возможно, если их признаковые области пересекаются. Причем изменяются, прежде всего, совпадающие признаки. Но так как между признаками объекта существуют связи, то через них происходит изменение других (несовпадающих) признаков. Таким образом происходит обучение живых существ — объектов материального мира с гибкой признаковой структурой.

Человек получает информацию от взаимодействующего другого человека и объекта тогда, когда у него есть идентичные с ними признаки или он способен расширить свою признаковую структуру за счет новых признаков (способен к обучению). Ребенок при рождении имеет признаковую структуру, определяемую его генетическим кодом и воздействиями во время внутриутробного развития. Во время жизни меняется его признаковая структура не только за счет антрометрических и физиологических признаков, но и за счет, прежде всего, признаков структуры мозга и его элементов. На основе анализа воспоминаний больных, воспроизводимых во время нейрохирургических операций, ученые пришли к выводу, что человек запоминает всю информацию, которая воспринимается его

органами чувств. Так как информация у человека отображается в структурах веществ его мозга, то при каждом взаимодействии его органов чувств с внешними объектами мира изменяется признаковая структура мозга. Но в каждый момент времени запоминаются только приращения знаний по отношению к знаниям в предшествующие моменты времени. Следовательно, информацию представляют не сами знания, а их приращения. Такой метод записи информации, известный как Δ-модуляция, существенно более экономный и широко используется в связи.

Так как информация нематериальна, то для ее хранения и передачи энергия не нужна. Очень малые количества вещества (катализаторы, гомеопатические лекарства) могут существенно влиять на химические реакции других веществ, недаром говорят, что слово может «убить» человека. Лауреат Нобелевской премии врач-гомеопат Джордж Витулкас успешно лечит людей гомеопатическими препаратами столь высокого разведения водой, что в них отсутствуют молекулы лекарственных исходных веществ. Этот феномен объясняют тем, что вода запоминает структуру растворенных в ней веществ и приобретает их свойства при сколь угодно большом разведении. Поэтому попытки объяснить паранормальные (ясновидение, телепатия и др.) явления на основе закона сохранения энергии некорректны. Можно предположить, что в множестве фактов об этих явлениях, от которых нельзя просто отмахнуться, проявляются пока неизвестные носители информации.

Так как информация отражает свойства материальных объектов и отношения между ними, то в соответствии с основными понятиями философии [3] информацию можно отнести к **предмету познания**, а защищаемую информацию — к **предмету защиты**.

Защите подлежит секретная и конфиденциальная информация. К секретной относится информация, содержащая **государственную тайну**. «Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» [4].

Под **конфиденциальной** понимается информация с ограниченным доступом, не содержащая государственную тайну. В [5]

дается следующее ее определение: информация конфиденциальная — служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной тайне, государственной службе и других законодательных актов. В соответствии с Указом Президента РФ № 188 от 06.03.1997 г. к конфиденциальной информации относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных сообщений и т. д.);
- сведения, связанные с коммерческой деятельности, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами;
- сведения о существе изобретения (идеи конструкторской разработки или промышленного образца) до официальной публикации информации о нем.

Но к коммерческой тайне не могут быть отнесены:

- сведения, охраняемые государством;
- общеизвестные и общедоступные сведения, патенты, товарные знаки;
- сведения о незаконной и негативной стороне деятельности коммерческих организаций;
- учредительные документы и сведения о хозяйственной деятельности.

Без информации не может существовать жизнь в любой форме и не могут функционировать созданные человеком любые информационные системы. Без нее биологические и искусственные сис-

темы представляют груду химических элементов. Опыты по изоляции органов чувств человека, затрудняющие информационный обмен человека с окружающей средой, показали, что информационный голод (дефицит информации) по своим последствиям не менее разрушителен, чем голод физический. Несмотря на определенные достижения прикладной области науки — информатики, занимающейся информационными процессами, достаточно четкого понимания сущности информации наука пока не имеет.

## 3.2. Виды защищаемой информации

Любая информация содержится на материальных носителях в виде значений их признаков, т. е. она отображается на носителях информации на языке признаков. Язык признаков является универсальным языком представления информации в материальном мире. Информация, отображаемая на языке признаков, называется **признаковая**. Информация признаковая является первичной и описывает конкретный материальный объект на языке его признаков. Описание объекта содержит признаки его внешнего вида, излучаемых им полей и элементарных частиц, состава и структуры веществ, из которых состоит объект. Источниками признаковой информации являются сами объекты. К ним в первую очередь относятся интересующие зарубежную разведку или отечественного конкурента люди, новая продукция и материалы, помещения и даже здания, в которых может находиться конфиденциальная информация. В зависимости от вида описания объекта признаковая информация делится на информацию о внешнем виде (видовых признаках), о его полях (признаках сигналов), о структуре и составе его веществ (признаках веществ).

Признаки принадлежат конкретному объекту, но их значения могут отражать как свойства самого объекта, так и результаты взаимодействия рассматриваемого объекта с другими. Например, значения признаков отраженного от объекта света содержат признаки внешнего источника света, поверхности объекта и среды распространения лучей света от его источника до оптического приемника. Изображение объекта на фотографии представляет модель объекта, которая с той или иной степенью приближения может соответствовать реальному объекту. Усилия создателей фототехники

направлены на увеличение степени подобия изображения реальному объекту. Однако это подобие достигается усложнением фотообъектива и повышением качества фотопленки, что увеличивает стоимость фотографии.

**Семантическая информация по отношению к признаковой является вторичной**, синтезируемой второй сигнальной системой человека в результате кодирования признаков символами. Когда человек читает текст книги, его зрительный анализатор сканирует поверхность листа и выделяет видовые признаки текста, а вторая сигнальная система формирует текущие признаковые структуры символов (букв, цифр, слов) и распознает символы в результате идентификации их текущих признаковых структур с эталонными структурами. Если человек не обучен иностранному языку, то в его памяти отсутствуют эталонные признаковые структуры букв и слов иностранного языка, и он не понимает текст в книге.

Если признак привязан к конкретному объекту, то символьная (семантическая) информация абстрактна. Сущность семантической информации не зависит от характеристик носителя. Содержание текста, например, не зависит от качества бумаги, на которой он написан, или физических параметров другого носителя. **Семантическая информация — продукт абстрактного мышления человека и обработки данных рецепторов других живых существ**. Семантическая информация, циркулирующая в человеческом обществе, отображает создаваемые ими образы и модели с помощью символов на языках общения людей.

Языки общения включают как естественные языки национального общения, так и искусственные профессиональные языки. Любой язык включает набор символов — алфавит и правила их использования — грамматику.

**Языки национального общения** формируются в течение длительного времени развития нации. В нем устаревшие слова постепенно отмирают, но появляются новые, вызванные развитием нации, в том числе техническим прогрессом.

Семантическая информация на языке национального общения представляется в виде упорядоченной последовательности символов (букв, цифр, иероглифов) алфавита этого языка и записывается на любом материальном носителе. В области средств регистрации

и консервации семантической информации изыскиваются носители, обеспечивающие все более высокую плотность записи и меньшее энергопотребление.

**Профессиональные языки** создаются специалистами для экономного и компактного отображения информации. Существует множество профессиональных языков: математики, музыки, радиоэлектроники, автодорожного движения, химии и т. д. Любая предметная область содержит характерные для нее понятия и условные обозначения, часто непонятные необученному этому языку человеку. Для однозначного понимания этого языка всеми специалистами областей науки, техники, искусства и др. термины и условные обозначения стандартизируются. В принципе все то, что описано на профессиональном языке, можно представить на языке общечеловеческого общения, но такая форма записи громоздка и неудобна для восприятия информации человеком. Кроме того, использование носителей различной физической природы позволяет подключать для ввода информации в мозг человека все многообразие его рецепторов (датчиков). При просмотре кинофильмов, например, основной объем информации зритель получает через органы зрения. Музыкальное сопровождение фильма через слуховой канал ввода информации оказывает дополнительное воздействие на эмоциональную сферу зрителя. Известны попытки дополнить эти каналы воздействием на органы обоняния человека путем создания в кинозале соответствующих запахов. В ситуациях, когда нельзя использовать для информирования человека зрительные или акустические сигналы или эти каналы перегружены, воздействуют на его тактильные рецепторы. Например, нательное средство для обнаружения записывающего устройства в кармане собеседника или сотовый телефон информируют о работе с помощью вибрации.

## 3.3. Демаскирующие признаки объектов защиты

Задача защиты признаковой информации решается, прежде всего, путем предотвращения обнаружения и распознавания признаков объектов, по которым можно обнаружить и распознать объекты, т. е. найти эти объекты среди других объектов, определить их назначение, задачи, функции и характеристики. Признак объ-

екта, позволяющий обнаруживать и распознавать объект, которо му принадлежит признак, среди других объектов, называется де маскирующим.

### 3.3.1. Классификация демаскирующих признаков объектов защиты

Классификация демаскирующих признаков по различным основаниям дана на рис. 3.1.

В зависимости от состояния объекта его демаскирующие признаки разделяются на **опознавательные признаки** и **признаки деятельности**.

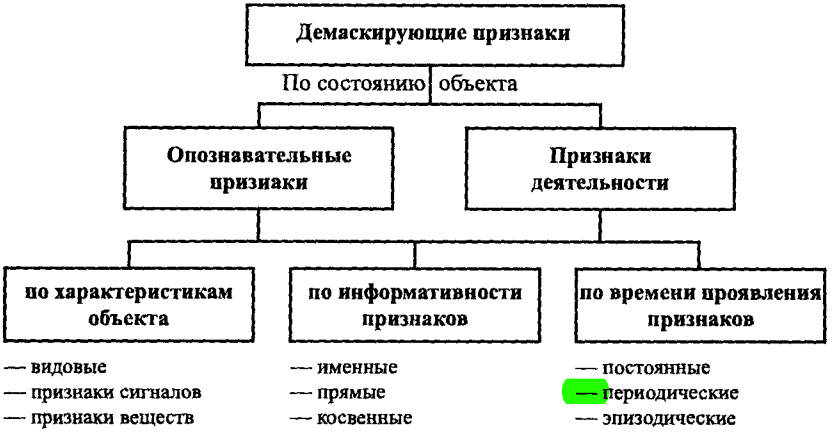



*Рис. 3.1.* Классификация демаскирующих признаков

**Опознавательные признаки** описывают объекты в статическом состоянии: его внешний вид, излучения, физические и химические свойства и др. **Признаки деятельности** объектов характеризуют этапы и режимы функционирования объектов. Например, этапы создания новой продукции включают: научные исследования, подготовку к производству, изготовление новой продукции, ее испытания и т. д. Признаки деятельности представляют собой последовательность во времени событий или действий составных элементов рассматриваемого объекта и взаимодействующих с ним объектов, а также значения статистических характеристик событий и действий. Например, по активности посещения студентами библиотек и их количеству в читальном зале можно спрогнозиро-

вать время сдачи курсового проекта, зачета или экзамена. По активности работы средств радиосвязи войсковой части можно определить вид их деятельности: повседневная деятельность в местах постоянной дислокации, подготовка к передислокации, перемещение, развертывание в месте новой дислокации.

Демаскирующие признаки объекта можно разделить на три группы:

- видовые признаки;
- признаки сигналов;
- признаки веществ.

К видовым признакам относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

Признаки сигналов описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.

Признаки веществ определяют физический и химический состав, структуру и свойства веществ материального объекта.

Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет собой модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Важнейшим показателем признака является его **информативность**. Информативность признака оценивается мерой в интервале [0–1], характеризующей его индивидуальность. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен. Величину информативности можно определить как $I_k = (N - N_k) / N$, где $N_k$ — количество объектов, содержащих признак к, из N рассматриваемых. Если признак принадлежит одному объекту, то информативность максимальная и приближается к 1; если признак принадлежит всем объектам выборки, то информативность нулевая. Информативность конкретного k-го признака можно характеризовать вероятностью $P_k$ обнаружения конкретного объекта по этому признаку среди других рассматриваемых объектов.

Наиболее информативен **именной** признак, присущий одному конкретному объекту. Такими признаками являются фамилия, имя, отчество человека, папиллярный рисунок его пальцев, инвен-

тарный номер прибора или образца мебели. Факты, например, о совпадении папиллярных узоров пальцев хотя бы двух разных людей не известны.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых **прямыми**, колеблется в пределах [0–1]. Признаки, непосредственно не принадлежащие объекту, но отражающие его свойства и состояние, называются **косвенными**. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Следы краски или характер деформации поверхности автомобиля в результате автодорожного происшествия позволяют находить автомобиль, скрывшийся с места происшествия. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако если в результате взаимодействия объектов на одном из них появляются именные признаки другого объекта, то информативность косвенного признака может приближаться к 1, например, четкие отпечатки пальцев на предметах, следы обуви, протектора шин машины и др.

По времени проявления признаки могут быть:

- постоянными, не изменяющимися или медленно меняющимися в течение жизненного цикла объекта;
- периодическими, например следы на снегу;
- эпизодическими, проявляющимися при определенных условиях, например случайно появившееся на поверхности объекта пятно краски.

Каждый k-й признак обеспечивает возможность обнаружения объекта с вероятностью $P_k$, при увеличении количества используемых признаков вероятность обнаружения и распознавания повышается. Если признаковая структура содержит n независимых признаков, то вероятность обнаружения объектов с помощью этих признаков повышается до величины $Q_n = 1 - \prod_{k=1}^{n} (1 - P_k)$. Например, если $P_1 = 0{,}05$, $P_2 = 0{,}1$, $P_3 = 0{,}15$, $P_4 = 0{,}2$ и $P_5 = 0{,}25$, то вероятность

обнаружения объекта хотя бы по одному из этих признаков существенно выше — более 0,56.

Если признаки зависимы, т. е. проявление какого-либо признака статистически связано с проявлением другого, то вероятность обнаружения объекта уменьшается по сравнению с вариантом независимых признаков. Например, значения признака «тень» при наблюдении объекта зависят от значения признака «размеры» и от взаимного пространственного положения объекта и внешнего источника света. Для повышения вероятности обнаружения и распознавания объекта стремятся увеличить количество информативных независимых признаков. Так же как информативность одного признака характеризует вероятность обнаружения объекта по этому признаку, то информативность признаковой структуры соответствует вероятности обнаружения объекта по признакам признаковой структуры объекта. Поэтому информативность признаковой структуры определяется по закону сложения вероятностей. Для n независимых признаков она равна:

$$I_{пс} = \sum_{k=1}^{n} I_k - \sum_{k<l} I_k I_l + \sum_{k<l<m} I_k I_l I_m + \cdots + (-1)^{n-1} I_1 I_2 \ldots I_n,$$

где $I_k$ — информативность k-го признака.

Например, информативность признаковой структуры с 3 признаками, информативность каждого из которых $I_1 = 0{,}1$; $I_2 = 0{,}2$; $I_3 = 0{,}3$, равна $I_{пр} = 0{,}496$.

Структуры с наиболее достоверными априорными признаками объекта называются **эталонными**, а структуры с полученными в момент наблюдения и измерения признаками — **текущими**. Эталонные структуры периодически корректируются путем замены их недостаточно достоверных признаков более достоверными и информативными текущими признаками. Например, фотография в паспорте как эталонная признаковая структура видовых признаков лица владельца заменяется на новую при изменении информативных значений признаков в результате старения, отпускания бороды и усов, вживления волос на облысевшую часть головы, изменения черт лица после пластической операции.

### 3.3.2. Видовые демаскирующие признаки

Видовые демаскирующие признаки описывают внешний вид объекта. Они объективно ему присущи, но выявляются в результате анализа внешнего вида модели объекта — его изображения на экране оптического приемника (сетчатки глаза человека, фотоснимке, экрана телевизионного приемника, прибора ночного видения и т. д.). Так как модель в общем случае отличается от оригинала, то состав и значения видовых демаскирующих признаков зависят не только от объекта, но и от условий наблюдения и характеристик оптического приемника.

Наибольшее количество информативных видовых демаскирующих признаков добывается при визуально-оптическом наблюдении объектов в видимом диапазоне.

Основными видовыми демаскирующими признаками объектов в видимом свете являются:

- фотометрические и геометрические характеристики объектов (форма, размеры объекта, цвет, структура, рисунок и детали его поверхности);
- тени, дым, пыль, следы на грунте, снеге, воде;
- взаимное расположение элементов группового (сложного) объекта;
- расположение защищаемого объекта относительно других известных объектов.

Геометрические и фотометрические характеристики объектов образуют наиболее устойчивую и информативную информационную структуру, так как они присущи объекту и относятся к прямым признакам.

Размеры объекта наблюдения определяются по максимальному и минимальному линейным размерам, площади и периметру проекции объекта и его тени на плоскость, перпендикулярную к линии визирования (наблюдения), высоте объекта и др. Размеры приобретают значение основного демаскирующего признака для объектов примерно одинаковой формы.

Форма — один из основных демаскирующих признаков, прежде всего искусственных объектов, поскольку для них, как правило, характерны правильные геометрические формы.

Детали объектов, их количество, характер расположения дают представление о сложном объекте и позволяют отличить его от подобных по форме.

Тени объектов возникают в условиях прямого солнечного освещения и являются важными демаскирующими признаками объекта при наблюдении его сверху. Некоторые объекты (например, линии электропередачи, антенные мачты, ограждения и т. д.) часто распознают только по тени. Различают два вида тени: собственную, от элементов объектов, которая ложится на поверхность самого объекта, и падающую, отбрасываемую объектом на фон. По падающей тени можно обнаружить объект, определить его боковые размеры, высоту, а также в ряде случаев и форму.

Важнейшим свойством поверхности объекта, определяющим его цвет и яркость, является коэффициент отражения поверхности для различных длин волн и частот: в видимом, инфракрасном и радиодиапазоне.

Объекты по-разному отражают падающие на них лучи света. Например, коэффициент отражения листвы летом в ближнем инфракрасном диапазоне в 3–5 раз выше, чем в видимом, а у бетонных и асфальтовых покрытий отличаются незначительно.

Отражательные свойства объектов описываются коэффициентами (спектральными и интегральным) и индикатрисой отражения. Индикатриса отражения характеризует распределение силы отраженного света в пространстве. Интегральный коэффициент отражения определяется в результате усреднения спектральных (на одной длине волны) коэффициентов отражения в рассматриваемом диапазоне длин волн.

В зависимости от характера поверхности различают **направленное (зеркальное)**, **рассеянное (диффузное)** и **смешанное отражения**. Граница между ними условная и определяется соотношением величин неровностей поверхности и длины падающей волны. Поверхность считается гладкой и отражение от нее зеркальное, если отношение среднеквадратичного значения высоты неровностей h к длине волны $\lambda$ менее единицы, шероховатой с диффузным отражением, если более двух. Следовательно, шероховатая поверхность в видимом свете может в ИК-диапазоне выглядеть как гладкая. Диффузное отражение присуще мелкоструктурным элемен-

там, таким как песок, свежевыпавший снег. Большинство объектов земной поверхности имеют смешанную индикатрису отражения.

Яркость объекта, определяемая не только коэффициентами отражения объекта, но и яркостью внешнего источника освещения, относится к косвенным признакам, таким как дым, пыль, его следы на различных поверхностях.

Любые тела излучают электромагнитные волны в ИК-диапазоне. Величина энергии, излучаемая любым телом с температурой T, пропорциональна в соответствии с формулой Стефана—Больцмана величине $T^4$. В ближней (0,75–1,3 мкм) и средней (1,2–3,0 мкм) зонах ИК-излучения мощность теплового (собственного) излучения объектов значительно меньше мощности отраженного от объекта потока солнечной энергии. С переходом в длинноволновую область ИК-диапазона мощность собственного излучения нагретых Солнцем объектов становится соизмеримой с мощностью отраженной ими солнечной энергии. Максимум энергии ИК-излучения тел при температуре воздуха летом находится в диапазоне 3–5 и 8–14 мкм. Чем выше температура тела, тем больше излучаемая энергия, а ее максимум смещается в сторону более коротких волн. Поэтому нагретые тела с помощью соответствующих приборов могут наблюдаться в полной, с точки зрения человека-наблюдателя, темноте.

При оценке излучений в инфракрасном диапазоне необходимо учитывать теплопроводность материалов объектов наблюдения. Нагреваясь от солнечных лучей, они к отраженному свету добавляют повышающуюся с ростом температуры долю собственных излучений. В связи с этими свойствами в инфракрасном диапазоне появляется дополнительный признак — температура различных участков поверхности объекта по отношению к температуре фона.

Зрительный анализатор человека не воспринимает лучи в инфракрасном диапазоне. Поэтому видовые демаскирующие признаки в этом диапазоне добываются с помощью специальных приборов (ночного видения, тепловизоров), имеющих худшее разрешение, чем глаз человека. Кроме того, видимое изображение на экранах этих приборов одноцветное. Но изображение в инфракрасном диапазоне может быть получено при малой освещенности объек-

та или даже в полной темноте, а к демаскирующим признакам добавляются признаки, характеризующие температуру поверхности объекта.

В общем случае к демаскирующим признакам объекта в ИК-диапазоне относятся:

• геометрические характеристики внешнего вида объекта (форма, размеры, детали поверхности);

• температура поверхности.

В радиодиапазоне наблюдается более сложная картина, чем при отражении света. Отражательные возможности поверхности в этом диапазоне определяются, кроме указанных для света, ее электропроводностью и конфигурацией относительно направления падающей волны. Большая часть суши отражает электромагнитную волну в радиодиапазоне диффузно, спокойная водная поверхность — зеркально.

Радиолокационное изображение объектов сложной формы (автомобиль, самолет и др.) формируется совокупностью отдельных пятен различной яркости, соответствующих так называемым «блестящим точкам»» объектов, отражающих сигнал в направлении радиолокационной станции (РЛС). «Блестящие точки» на экране локатора создают элементы поверхности объектов, расположенные перпендикулярно направлению облучения, а также элементы конструкции, которые после переотражений радиоволн внутри конструкции возвращают их к радиолокатору.

Наибольшей отражающей способностью в направлении антенны радиолокационной станции обладают конструкции в виде 2–4 жестко связанных между собой взаимно перпендикулярных металлических или металлизированных плоскостей. Такие конструкции называются **уголковыми радиоотражателями**, применяемыми для имитации ложных объектов.

Конкретный вид радиолокационного изображения зависит от положения объекта относительно направления облучения, так как при изменении ориентации меняется количество и взаимное положение «блестящих точек». Обобщенные результаты анализа радиолокационных изображений местности и объектов приведены в табл. 3.1 и 3.2 [6].

*Таблица 3.1*

| *Вид отражающей поверхности* | *Характер отражения* | *Тон радиолокационного изображения* |
|---|---|---|
| Водная в тихую погоду | Гладкая водная | Темный |
| Травяной покров | Диффузный, умеренной интенсивности с понижением ее при уменьшении электропроводности | Умеренно темный |
| Отдельные группы деревьев | Диффузный, высокой интенсивности | Светлый, с зернистой структурой |
| Естественные уголковые отражатели (скальные выступы, рвы) | Интенсивный | Очень светлый |
| Сельскохозяйственные угодья | Диффузный, различной интенсивности | От умеренно-темного до светлого |

*Таблица 3.2*

| *Объекты* | *Интенсивность отражения* | *Характер радиолокационного отражения* |
|---|---|---|
| *1* | *2* | *3* |
| Шоссейные дороги | Низкая | Линии с характерными изгибами, по тону слабо отличаются от окружающей местности |
| Железные дороги | Низкая | Линии с характерными изгибами |
| Мосты, переправы | Высокая | Короткий прямой светлый отрезок поперек реки |
| Промышленные объекты | Высокая | Площадь светлого тона с резкими границами |
| Силовые линии электропередач | Высокая (от металлических опор) | Линейное расположение светлых точек |

| 1 | 2 | 3 |
|---|---|---|
| Аэродромы, ВПП, аэродромные постройки | От поверхности аэродрома и ВПП — низкая, от построек — высокая | Площадь аэродрома умеренно-темная, ВПП и постройки — темные |
| Самолеты и другая техника | Высокая | Отдельные светлые точки, расположенные на местности в определенном порядке |

*Примечание.* ВПП — взлетно-посадочная полоса аэродрома.

Отражательная способность объекта в радиодиапазоне характеризуется эффективной поверхностью (площадью) рассеяния (ЭПР). **Эффективная поверхность рассеяния (отражения)** соответствует площади металлической поверхности гипотетического объекта, который равномерно отражает во все стороны электромагнитную волну радиолокационной станции, а размещенный в месте нахождения реального объекта создает у приемной антенны радиолокационной станции такую же плотность потока мощности, как и реальный объект. Следовательно, реальный объект заменяется моделью с определенной поверхностью рассеяния, интегральные отражательные свойства которой соответствуют реальному объекту. Так как энергия отраженной волны зависит от конфигурации поверхности облучаемого объекта, то значения его ЭПР имеют для одного и того же объекта большой разброс, зависящий от положения объекта относительно направления на радиолокационную станцию. Эффективная поверхность рассеяния человека составляет около 0,1–0,5 м$^2$, легкового автомобиля — около 1–5 м$^2$, грузового автомобиля 3–10 м$^2$.

Так как частота колебаний электромагнитного поля радиолокационной станции велика (в 3-см диапазоне составляет около 10 ГГц), то в силу поверхностного эффекта в отражении электромагнитной волны принимает участие тонкий слой (порядка 0,01 мм) металлической поверхности объекта. Чем хуже электрическая проводимость объекта отражения, тем ниже коэффициент отражения и глубже проникает электромагнитная волна. Проникающая способность в дециметровом диапазоне для сухой почвы, например, может составлять 1–2 м. Отражение радиоволн сантиметрового

диапазона от бетона слабее, чем от металла, в 3–5 раз, а от кирпичной кладки — в 8–10 раз.

Отражающая способность земной поверхности изменяется в широких пределах в зависимости от ее шероховатости, диэлектрической проницаемости материала и длины волны. Средняя удельная (деленная на геометрическую площадь облучаемой поверхности) ЭПР песчаной почвы составляет 0,003, луга летом — 0,01, кустарника — 0,03, лесного массива — 0,05 [7].

К основным видовым демаскирующим признакам объектов радиолокационного наблюдения относятся:

- эффективная поверхность рассеяния;
- геометрические и яркостные характеристики (форма, размеры, яркость, детали);
- электропроводность поверхности.

Видовые демаскирующие признаки в радиодиапазоне добываются также с помощью тепловой радиолокации, приемники которой способны принимать сигналы собственных электромагнитных излучений и формировать на их основе изображения объектов. Так как возможности радиолокаторов, в особенности тепловых, весьма ограничены по разрешению, то в радиодиапазоне выявляется меньший, чем в видимом диапазоне набор демаскирующих признаков.

Таким образом, максимальное количество признаков внешнего вида объектов добывают в видимом оптическом диапазоне фотоприемники с высоким разрешением, к которым в первую очередь относятся глаз человека и фотопленка.

В инфракрасном и радиодиапазонах отсутствует такой информативный признак как цвет. С увеличением длины волны ухудшается разрешение значений признаков, например точность оценки размеров объекта и его деталей. Если в инфракрасном диапазоне по изображению можно измерять объекты на местности с точностью до долей мм, то максимальное разрешение радиолокационных станций составляет единицы метров. Поэтому на радиолокационном изображении будут отсутствовать многие детали объекта, наблюдаемые на его изображении в оптическом диапазоне. Однако в инфракрасном и радиодиапазонах проявляются дополнительные признаки, которые в видимом диапазоне отсутствуют.

Следовательно, видовые демаскирующие признаки объектов образуют признаковые структуры, отличающиеся в различных диапазонах длин электромагнитных волн. Эти свойства видовых демаскирующих признаков используются при комплексном добывании информации и их необходимо учитывать при организации защиты.

Любой объект наблюдения можно рассматривать как сложный объект, состоящий из более простых объектов, содержащих не только свои демаскирующие признаки, но и демаскирующие признаки сложного объекта. Например, прибор состоит из блоков, блоки из узлов и т. д. Новые оригинальные детали, узлы, блоки, придающие прибору новые свойства и параметры, представляют собой демаскирующие объекты, по внешнему виду которых можно не только обнаружить прибор, но и определить его характеристики. Вычленение из объекта защиты демаскирующих объектов позволяет решать вопросы защиты информации о нем путем защиты информации о демаскирующих объектах. Это часто бывает сделать проще и на более высоком уровне безопасности информации. Например, демаскирующие объекты можно хранить и перевозить отдельно от других частей изделия, а собирать изделие на месте его эксплуатации. Демаскирующие объекты классифицируются по информативности на именные, прямые и косвенные, по времени проявления — постоянные, периодические и эпизодические.

### 3.3.3. Демаскирующие признаки сигналов

Понятие «сигнал» достаточно емкое и в общем случае обозначает изменяющуюся физическую величину, однозначно отображающую сообщение. Часто люди для передачи конфиденциальной информации обмениваются условными сигналами, используя для этого различные предметы, надписи, слова, звуки. Например, незнакомые люди при встрече обмениваются условными фразами. В радиоэлектронике под сигналом понимается изменяющаяся физическая величина.

По существу сигнал представляет распространяющийся в пространстве носитель с информацией, содержащейся в значениях его физических параметров. К сигналам относятся: собственные (обусловленные тепловым движением электронов, радиоактивные) из-

лучения объектов, отраженные от объектов поля и волны, электромагнитные поля и электрический ток от созданных человеком источников сигналов. **Информация, содержащая в любом сигнале, представлена значениями его информационных параметров.** Классификация сигналов представлена на рис. 3.2.


*Рис. 3.2.* Классификация сигналов

К аналоговым сигналам относятся сигналы, уровень (амплитуда) которых может принимать произвольные значения в определенном для сигнала интервале.

Амплитуда простого и достаточно распространенного в природе гармонического сигнала изменяется по синусоидальному закону:

$$s(t) = A\sin(\omega t + \varphi),$$

где A — амплитуда; $\omega = 2\pi f$ — круговая частота колебания; $\varphi$ — фаза колебания.

Частота f измеряется в Гц и называется линейной.

Большинство аналоговых сигналов имеют более сложную форму. Периодические (повторяющиеся через время $T_п$ — период) сигналы произвольной формы могут быть представлены в соответствии с формулой Фурье в виде суммы гармонических колебаний:

$$s(t) = C_0 + \sum_{k=1}^{n} C_k \cos(k\omega_1 t - \varphi_k),$$

где $C_0$ — постоянная составляющая сигнала; $C_k$ — амплитуда k-й гармоники сигнала (k = 1, 2, ..., n); $k\omega_1$ и $\varphi_k$ — частота и фаза k-й гармоники сигнала; $\omega_1$ — основная (1-й гармоники), частота.

Параметры ряда Фурье вычисляются по соответствующим формулам, например [8]. Ряд Фурье представляет собой математическую модель периодического сигнала, так же как любой цвет может быть разложен на составляющие красного, зеленого и синего цветов. Совокупность гармонических (спектральных) составляющих сигнала образует его **спектр**.

Амплитуда каждой спектральной составляющей характеризует энергию соответствующей гармоники основной частоты сигнала. Чем выше скорость изменения амплитуды сигнала, тем больше в его спектре высокочастотных гармоник. Разность между максимальной и минимальной частотами спектра сигнала, между которыми сосредоточена основная часть, например 95% энергии, называется **шириной спектра** $\Delta F$. Пример графического изображения спектра периодического сигнала представлен на рис. 3.3.

Частоты составляющих спектра непериодического аналогового сигнала непрерывно меняются. При наблюдении спектра такого сигнала на экране анализатора спектра положение и уровень различных спектральных составляющих непрерывно изменяются и спектр выглядит как сплошной.

Весьма удобной и широко применяемой является комплексная форма записи ряда Фурье, которая в соответствии с формулой Эйлера определяет тригонометрические функции через показательные: $\cos x = (e^{jx} + e^{-jx}) / 2$ и $\sin x = (e^{jx} - e^{-jx}) / 2j$. Представление сигнала в виде ряда Фурье в комплексной форме имеет вид: $s(t) = \sum_{k=-n}^{k=n} C_k^* e^{jk\omega_1 t}$. Как следует из приведенного выражения, спектр в комплексной форме, называемый линейчатым, симметричен относительно нуля, а $C_k^* = 1/2\ C_k$ для $k \neq 0$.

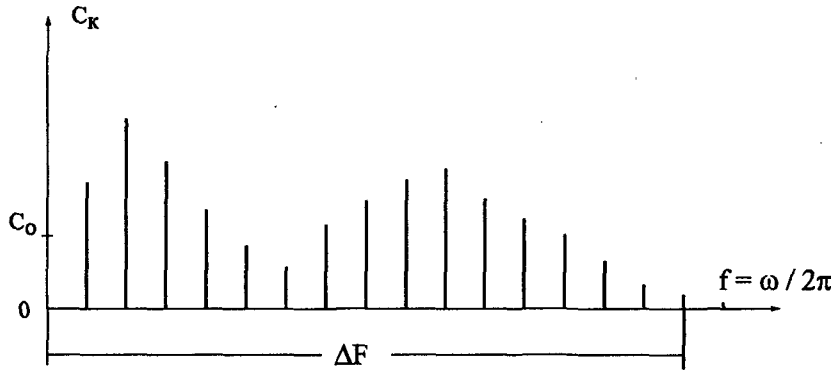



*Рис. 3.3.* Пример спектра периодического аналогового сигнала

В соответствии с изменением амплитуды аналогового сигнала меняется его энергия или мощность, пропорциональная квадрату амплитуды. В зависимости от времени измерения энергии сигнала различают **среднюю** и **мгновенную мощность**. Десятичный логарифм отношения максимальной мгновенной мощности сигнала к минимальной называется **динамическим диапазоном сигнала**. Динамический диапазон речи диктора радио и телевидения составляет 25–30 дБ, вокального ансамбля — 45–65 дБ, а симфонического оркестра достигает 70–95 дБ.

Аналоговый сигнал описывается набором параметров, являющихся его признаками. К ним относятся:

- частота или диапазон частот;
- амплитуда или мощность сигнала;
- фаза сигнала;
- длительность сигнала;
- вид модуляции;
- ширина спектра сигнала;
- динамический диапазон сигнала.

У дискретных сигналов амплитуда имеет конечный, заранее определенный набор значений. Наиболее широко применяется двоичный (бинарный) дискретный сигнал: в ЭВМ, в телеграфии, при передаче данных. Информационные сигналы, циркулирующие в ЭВМ IBM PC, имеют два уровня амплитуды: низкий (L-уровень — 0 В) и высокий (H-уровень — 5 В). Осциллограмма бинарного сигнала показана на рис. 3.4.

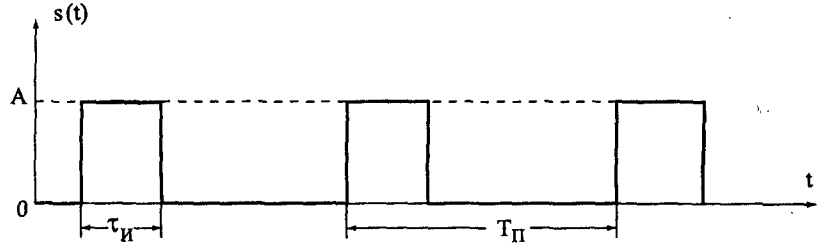



*Рис. 3.4.* Осциллограмма бинарного сигнала

Дискретный сигнал характеризуется следующими параметрами: амплитудой A и мощностью P, длительностью импульса $\tau_и$, периодом $T_п$ или частотой $F_п = 1 / T_п$ повторения импульсов (для периодических дискретных сигналов), шириной спектра сигнала $\Delta F_c$, скважностью импульсов $\alpha = T_п / \tau_и$.

Спектр дискретного периодического сигнала содержит бесконечное количество убывающих по амплитуде гармоник. Вид спектра для бинарного периодического сигнала иллюстрируется рис. 3.5.

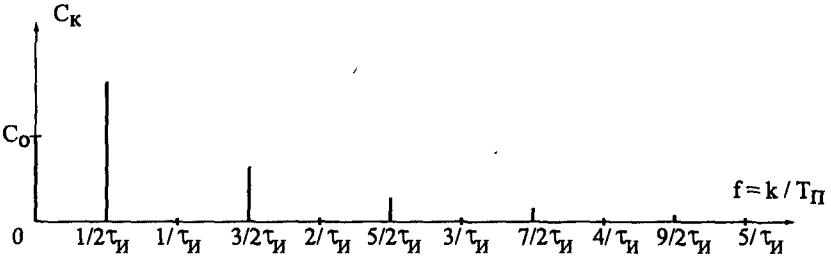



*Рис. 3.5.* Пример спектра бинарного периодического сигнала

Он характеризуется следующими свойствами:

- форма огибающей спектра описывается функцией $|\sin f/f|$;
- амплитуда гармоник $C_k$ имеет нулевое значение в точках $k / \tau_и$, $k = 1, 2, \ldots$;
- в области частот спектра $(0 - 1/\tau_и)$ располагаются $\alpha - 1$ гармоник;
- постоянная составляющая сигнала равна $A/\alpha$.

Учитывая, что большая часть энергии сигнала сосредоточена в области частот $0 - 1/\tau_и$, ширина спектра бинарного периодичес-

кого сигнала приблизительно оценивается по формуле: $\Delta F_и \approx 1/\tau_и$. Ширина спектра телеграфного сигнала в виде двоичной последовательности, ограниченного третьей гармоникой, оценивается величиной $\Delta F_т \approx 1{,}5v$, где v — скорость передачи в бодах (двоичных символах в секунду). Например, ширина спектра телеграфного сигнала, передаваемого со скоростью 50 Бод, приблизительно равна 75 Гц.

При прохождении дискретных сигналов по реальным электрическим цепям радиотехнических средств в силу их частотно-избирательных свойств и ограниченной полосы пропускания спектр сигналов изменяется, в результате чего искажается их форма и уменьшается крутизна импульсов. Прямоугольный импульс приобретает колоколообразную форму. В результате этого размывается граница между формами аналогового и дискретного сигналов. Искажения формы и уменьшение амплитуды импульсных сигналов в проводах кабелей ограничивают дальность их передачи, например, для обеспечения межмашинного обмена данными в локальных сетях.

По физической природе сигналы могут быть акустическими, электрическими, магнитными, электромагнитными (в радиодиапазоне — радиосигналы), корпускулярными (в виде потоков элементарных частиц) и вещественными, например, пахучие добавки в газ подают сигнал об его утечке.

Сигналы по виду передаваемой информации делятся на речевые, телеграфные, телекодовые, факсимильные, телевизионные, о радиоактивных излучениях и условные. Телеграфные и телекодовые сигналы используются для передачи буквенно-цифровой информации с низкой и высокой скоростью соответственно. Факсимильные и телевизионные сигналы обеспечивают передачу неподвижных и подвижных изображений. Сигналы радиоактивных излучений являются демаскирующими признаками радиоактивных веществ. Условные сигналы несут информацию, содержание которой предварительно определено между ее источником и получателем, например горшок с цветком на подоконнике в литературных произведениях о разведчиках — о провале явки.

Вид информации, содержащейся в сигнале, изменяет его демаскирующие признаки: форму, ширину спектра, частотный и

динамический диапазон. Например, стандартный речевой сигнал, передаваемый по телефонной линии, имеет ширину спектра 300–3400 Гц, звуковой — 16–20000 Гц, телевизионный — 6–8 МГц и т. д. Произведение $B = \Delta F_c T_c$ называется **базой сигнала**. Если $B \approx 1$, то сигнал узкополосный, при $B > 1$ — сигнал широкополосный.

По времени проявления сигналы могут быть регулярными, время появления которых получателю информации известно, например сигналы точного времени, и случайные, когда это время неизвестно. Статистические характеристики проявления случайных сигналов во времени могут представлять собой достаточно информативные демаскирующие признаки источников, прежде всего, об их принадлежности и режимах функционирования. Например, появление в помещении радиосигнала во время ведения в нем разговоров может с достаточно высокой вероятностью служить демаскирующим признаком закладного устройства с акустическим автоматом.

По аналогии с демаскирующим объектом и с такой же целью целесообразно ввести понятие **демаскирующий сигнал**, факт обнаружения которого может служить информативным признаком объекта защиты. Например, побочные излучения на определенной частоте конкретной радиостанции могут служить в качестве ее прямого, а иногда именного признака. Во время войны по «почерку» работы на ключе опознавали радиста и выявляли радиоигру, затеянную противником.

### 3.3.4. Демаскирующие признаки веществ

Потребительские свойства продукции зависят не только от конструктивных и схемотехнических решений, но и от свойств материалов (веществ), из которых она создается. Поэтому состав, свойства и технология получения веществ с этими свойствами вызывают большой интерес у специалистов, а информация о них может быть чрезвычайно дорогой.

**Веществом** называют материальные объекты в твердом, жидком или газообразном состоянии, состоящие из частиц одного или нескольких химических элементов, имеющие массу и объем. Классификация веществ приведена на рис. 3.6.

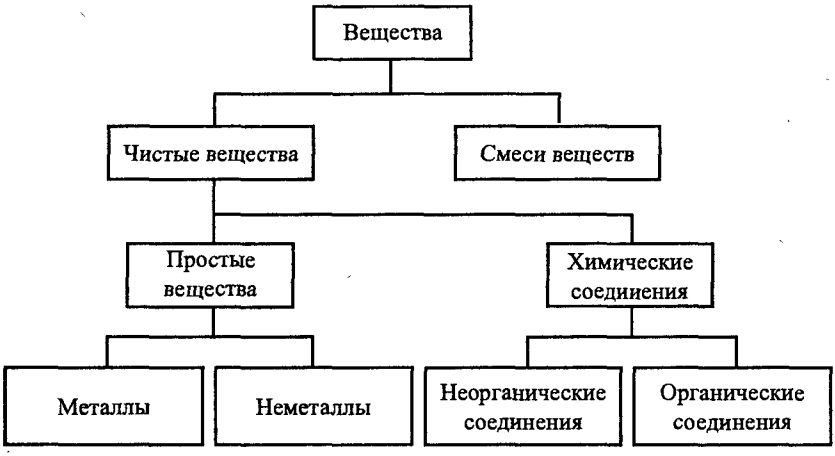



*Рис. 3.6.* Классификация веществ

Вещества делятся на простые и химические соединения (сложные). **Простые вещества** состоят из атомов одного химического элемента, **химические соединения** — из разных элементов. Химический элемент образуют атомы с одинаковым положительным зарядом ядра (с одинаковым порядковым номером в периодической системе Д. И. Менделеева). Атомы химических элементов могут существовать в свободном состоянии при очень высокой температуре или в составе простых веществ. Свойства химических соединений не совпадают со свойствами образующих его химических элементов.

По свойствам химические элементы условно делятся на **металлы и неметаллы**. К металлам относятся простые вещества, имеющие в обычных условиях кристаллическую структуру (кроме ртути), хорошую теплопроводность и электропроводность. В свою очередь металлы по плотности делятся на легкие (с плотностью до 5 г/см$^3$) и тяжелые, по температуре плавления — на легкоплавкие (с температурой плавления до 1000° С) и тугоплавкие, по химической стойкости к кислотам — благородные (серебро, золото) и неблагородные. Простые вещества, не обладающие признаками металлов, относятся к неметаллам.

Большинство соединений, в состав которых входит элемент углерод, относят к органическим. Но простейшие соединения уг-

лерода (оксиды — соединения из углерода и кислорода, угольная кислота и ее соли, некоторые другие), а также не содержащие углерод — к неорганическим соединениям.

Для обеспечения безопасности информации о веществах с новыми свойствами важно представлять признаки, по которым злоумышленник может воссоздать вещество с новыми свойствами. Классификация основных признаков веществ представлена на рис. 3.7.

По физическому составу вещества могут быть однородными **твердыми** (кусковыми, порошковыми), **жидкими, газообразными и неоднородными**, в виде взвесей, эмульсий и т. п.


*Рис. 3.7.* Классификация признаков веществ

По химическому составу вещества делятся на **органические и неорганические**. В свою очередь органические вещества — на углеводороды, кислородсодержащие и азотсодержащие, неорганические — на оксиды, кислоты, основания и соли.

**Изотопный** состав характеризует стабильность или нестабильность ядер веществ или, другими словами, наличие радиоактивных изотопов у рассматриваемого вещества.

***Ионный*** состав вещества определяется при нахождении его в ионизированном состоянии, называемой плазмой и возникающем под действием высокой температуры или газового разряда (для газообразных веществ).

Строение веществ описывают на **макроскопическом, микроскопическом и субмикроскопическом уровнях**. Оно может пред-

ставлять собой кристаллическую решетку, набор макромолекул, молекул, субатомных частиц и атомов.

**Механические** свойства веществ характеризуют их прочность на сжатие и растяжение, твердость, вязкость, плотность, пористость, пластичность, смачиваемость, непроницаемость и т. д.

**Химические** свойства вещества определяются по результатам взаимодействия его с другими веществами.

**Акустические** свойства определяют скорость передачи и поглощения звука в веществе.

**Тепловые** свойства оцениваются по температуре фазовых переходов из одного состояния в другое, теплопроводности, теплоемкости и др.

**Лучистые** (оптические, рентгеновские и др.) свойства вещества описываются коэффициентами и спектральными характеристиками пропускания, отражения, преломления, возможностями по дифракции, поляризации и интерференции лучей света в инфракрасном, видимом и ультрафиолетовом диапазонах, а также гамма-излучений.

Электропроводность, величины термо-ЭДС, окислительно-восстановительные потенциалы, потенциалы ионизации, диэлектрическая и магнитная проницаемость и т. п. характеризуют **электрические и магнитные** свойства вещества.

**Ядерные** свойства вещества оцениваются по массе изотопов, массе и периоду полураспада радиоактивных частиц и др.

Признаки, по которым можно обнаружить и распознать вещество, т. е. определить его состав, структуру и свойства, в смеси других веществ, являются **демаскирующими**. Демаскирующие признаки нового вещества и технологии его изготовления содержатся не только в конечном продукте, но и в исходных и промежуточных продуктах технологического процесса, применяемых для получения этого вещества. Вещество, содержащее демаскирующие вещественные признаки объекта защиты или технологию его изготовления, называют **демаскирующим веществом**. Например, новые духи отличаются от прототипов составом. Демаскирующими признаками новых духов являются характеристики запаха, а демаскирующими веществами — компоненты духов в определенном соотношении. Оригинальные духи отличаются от подделки так-

же рядом признаков, в том числе стойкостью сохранения запаха. Стойкость запаху придают специальные дорогие добавки, которые являются демаскирующими веществами оригинала. В результате физико-химического анализа демаскирующих веществ добывается информация о составе, структуре, свойствах и технологии изготовления продукции, которая может содержать государственную и коммерческую тайну.

Потенциальные возможности обнаружения и распознавания демаскирующих веществ зависят от их концентрации в смеси добываемых веществ. Минимально допустимые значения концентрации демаскирующих веществ, исключающие получение злоумышленниками защищаемой информации, используются в качестве норм при обеспечении безопасности информации о признаках веществ.

## 3.4. Свойства информации как предмета защиты

Для обеспечения эффективной защиты информации необходимо знать ее свойства. Она как предмет защиты обладает рядом свойств, основные из которых следующие:

1. Нематериальная информация может храниться, передаваться, обрабатываться, если она содержится на материальном носителе. Так как с помощью материальных средств можно защищать только материальный объект, **то объектами защиты являются материальные носители информации**. Различают носители — источники информации, носители — переносчики информации и носители — получатели информации. Например, чертеж является источником информации, а бумага, на которой он нарисован, — носитель информации. Физическая природа источника и носителя в этом примере одна и та же — бумага. Однако между ними существует разница. Бумага без нанесенного на ней текста или рисунка является источником информации о ее физических и химических свойствах. Когда бумага содержит семантическую информацию, то она становится документом — источником семантической информации. Некоторые романтические натуры пропитывают бумагу писем духами. Такое письмо содержит дополнительную информацию о запахе любимых духов автора.

Но независимо от вида информации, содержащейся на бумаге или ином другом носителе, защищать от хищения, изменения и уничтожения информации можно материальный объект — листы бумаги, которые имеют определенные размеры, вес, механическую прочность, устойчивость краски или чернил к внешним воздействиям и т. д., или иные носители. Параметры носителя определяют условия и способы хранения информации. Бумагу для обеспечения безопасности содержащейся на ней информации хранят в сейфе. Другие носители, например поля, не имеют четких границ в пространстве и их трудно запереть в шкаф. Но в любом случае характеристики материального носителя контролируемы органами чувств человека или его технических средств.

Параметры информации (затраты энергии, время передачи, стоимость и др.), которыми часто характеризуют ту или иную информацию, являются параметрами ее носителя. Энергетические затраты на передачу информации равны работе по перемещению носителя из одной точки пространства в другую. Для разных носителей эти затраты отличаются. Так же, например, время и энергия для передачи одной и той же информации по сети Интернет и на перекладных (на гужевом транспорте) несоизмеримы. Следовательно, физические характеристики информации представляют собой характеристики ее носителей.

2. **Информация может быть для ее для пользователя (собственника, владельца, получателя) достоверной и ложной, полезной и вредной**. Информация, отражающие объективные факты, события, явления и процессы, является **достоверной**, а не соответствующая им — **ложной**. Границу между достоверной и ложной информацией часто трудно провести. Достоверная информация в процессе передачи может трансформироваться в свою противоположность. Преднамеренно создаваемая и распространяемая ложная информация называется **дезинформацией**.

В естественных областях науки достоверной информацией считается та, которую может получить не только ее автор, но и другие ученые. Если результаты научного исследования не удается повторить, то информация считается недостоверной. Например, сенсационное сообщение английских физиков о получении ими «холодной» (при обычной температуре) термоядерной реакции снача-

ла вызвало большой интерес в мире, но после неудачных попыток повторить эксперимент другими учеными это сообщение было забыто.

Когда реальные факты интерпретируются людьми, то получаемая информация «окрашивается» их субъективизмом. Поэтому в гуманитарных областях науки могут существовать достаточно много разных, даже противоположных, точек зрения по одному и тому же вопросу. Достаточно сказать, что история, особенно не очень далекого времени, часто переписывается в угоду господствующему в данный период времени представлению об исторических событиях так называемой элиты. Трудность определения границы между достоверной и ложной информацией широко используется в информационных войнах, которые постоянно ведутся между не только государствами, но и различными группами и даже отдельными людьми. Какими бы независимыми себя не называли те или иные средства массовой информации, каждое из них объективно отражает лишь мнение своих владельцев или редакции. Оно отличается в различных соотношениях достоверной и ложной информации, доводимой до своих слушателей и читателей.

Полезная информация приносит прибыль ее владельцу или пользователю, уменьшает риск в его деятельности в результате принятия более обоснованных решений, улучшает его психическое состояние и т. д. Достоверная информация, как правило, является полезной, так как обеспечивает принятие более правильного решения. Но в отдельных случаях такая зависимость подвергается сомнению. Например, американские врачи сообщают больному о его неизлечимой болезни, так как считают, что такая информация позволяет больному принять более обоснованное решение о своих дальнейших действиях. Наши врачи часто скрывают правду, полагая, что такая информация может «добить» больного. Истина, как считают в таких случаях, посредине. Сильному человеку горькая правда полезна, так как она мобилизует его силы для борьбы с недугом, слабому более полезна «сладкая ложь», так как она поддерживает его жизненный тонус.

Вредной является информация, в результате использования которой ее получателю наносится моральный или материальный ущерб. Часто вредная информация создается в результате целенап-

равленной или случайной модификации ее при переносе с одного носителя на другой. Такая информация распространяется в виде **слухов**. Из этого не следует, что слухи содержат только ложную и вредную информации. Иногда власти допускают утечку достоверной информации с целью выявить реакцию общественности на готовящиеся непопулярные меры, а «звезды», особенно шоу-бизнеса, распускают слухи о себе для поддержания имиджа.

К вредной также относится информация, содержание которой является нейтральной для ее пользователя, но засоряет так называемое информационное пространство. Засоренность каналов связи и документов нейтральной информацией затрудняет и существенно увеличивает время добывания полезной. Многие по собственному опыту знают, как иногда трудно найти нужный документ в кипах других, от которых и пользы-то мало, но выбросить жалко. Кроме того, носитель с нейтральной для конкретного получателя информацией может оказывать вредное воздействие на другой носитель с полезной информацией, если близки по значениям параметры носителей, например частоты колебаний электромагнитных полей разных источников. Носители информации, оказывающее воздействие на другой носитель, представляют собой **помехи**. То, что для одного получателя является информацией, для другого — помеха. Когда во время разговора по телефону из-за неисправности в цепях коммутации телефонной станции слышен разговор других людей, то каждая пара абонентов воспринимает разговор другой как помеху.

Полезность информации всегда **конкретна**. Нет полезной информации вообще. Информация полезна или вредна для конкретного ее пользователя. Под пользователями подразумевается как один человек или автомат, так и группа людей и даже все человечество. Чрезвычайно полезная информация для одних пользователей может не представлять ценности для других. Даже информация, ценная для всего человечества, например технология изготовления лекарств от опасной болезни, для конкретного здорового человека может не представлять интерес.

Поэтому при защите информации определяют, прежде всего, круг лиц (фирм, государств), заинтересованных в защищаемой ин-

формации, так как вероятно, что среди них окажутся злоумышленники.

В интересах защиты ценной (полезной) информации ее владелец (государство, организация, физическое лицо) наносит на носитель условный знак полезности содержащейся на нем информации, — гриф секретности или конфиденциальности. Гриф секретности информации, владельцами которой является государство (государственные органы), устанавливается на основанин Закона «О государственной тайне» и ведомственных перечней сведений, составляющих государственную тайну. В соответствии с постановлением Правительства РФ № 870 от 4 сентября 1995 г. к информации секретной, совершенно секретной и особой важности относится информация, хищение или несанкционированное распространение которой может нанести ущерб соответственно государственной организации (предприятию, учреждению), отрасли (ведомству, министерству), субъекту Федерации и РФ в целом. Для несекретной информации, содержащей служебную тайну, вводят гриф «для служебного пользования».

Для обозначения степени конфиденциальности коммерческой информации применяют различные шкалы ранжирования. Наиболее распространена шкала: «строго конфиденциально», конфиденциально» и «не подлежит разглашению».

В качестве критерия для определения грифа конфиденциальности информации могут служить результаты прогноза последствий попадания информации к конкуренту или злоумышленнику.

Следствием разглашения или утери документа с грифом «строго конфиденциально» могут быть материальные и финансовые потери, которые могут привести организацию к банкротству или поглощению ее более мощной, а также к физическому и морально-психологическому воздействию на персонал организации. При попадании к конкуренту информации документов с грифом «конфиденциально» организации могут быть нанесены значительные материальные и финансовые потери. «Разглашению не подлежит» информация, представляемая в органы контроля, переписка, договоры, сведения о сотрудниках организации, воспользовавшись которыми злоумышленник может нанести им или организации вред.

3. Хотя информация нематериальная, она покупается и продается. Поэтому **информацию можно рассматривать как товар**. Полезность информации как товара характеризуется его ценой. Цена информации зависит от ее ценности, но это разные понятия. Например, при проведении исследований могут быть затрачены большие материальные и финансовые ресурсы, которые завершились отрицательным результатом, т. е. не получена информация, на основе которой ее владелец может получить прибыль. Но отрицательные результаты представляют ценность для специалистов, занимающихся рассматриваемой проблемой, так как полученная информация укорачивает путь к истине. Детские фотографии имеют большую ценность для родителей изображенных на них детей, но рыночная цена у них близка к нулю до тех пор, пока изображенный на фотографии ребенок не становится знаменитым. Цена фотографии знаменитого человека пропорциональна его рейтингу. Ценность информации — полезность ее для собственника (владельца, пользователя), цена — полезность информации для участников рынка.

Полезная информация может быть создана ее владельцем в результате научно-исследовательской деятельности, заимствована из различных открытых источников, может попасть к злоумышленнику случайно, например в результате непреднамеренного подслушивания, и, наконец, добыта различными нелегальными путями. Цена информации, как любого товара, складывается из себестоимости и прибыли.

Себестоимость определяется расходами владельца информации на ее получение путем:

- проведения исследований в научных лабораториях, аналитических центрах, группах, отдельными учеными и т. д.;
- покупки информации на рынке информации;
- добывания информации противоправными действиями.

Прибыль от информации ввиду ее особенностей может принимать различные формы, причем денежное ее выражение не является самой распространенной формой. В общем случае прибыль от информации может быть получена в результате следующих действий:

- продажи информации на рынке;

материализации информации в продукции с новыми свойствами или технологией, приносящими дополнительную прибыль;
использования информации для принятия более эффективных решений.

Последняя форма прибыли от информации не столь очевидна, но она самая распространенная. Это обусловлено тем, что любая деятельность человека есть по своей сути последовательность принятия им решений. Большинство решений принимается человеком бессознательно, он осознанно принимает в основном жизненно важные решения.

Для принятия любого решения нужна информация, причем, чем выше цена решения, тем большее количество ее необходимо. Размышления человека перед принятием решения представляют собой не что иное, как переработку человеком имеющейся у него информации. По своему опыту каждый знает, как трудно принять ответственное решение в условиях дефицита информации или времени.

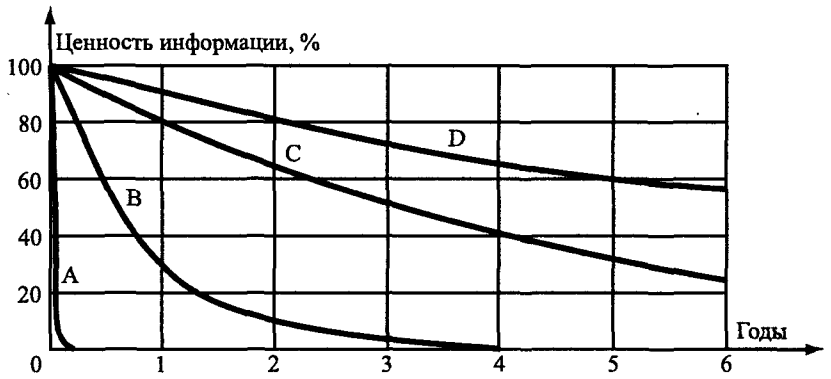
Дефицит времени при принятии решений возникает, когда недостаточно времени для восприятия (чтения) и обработки информации, необходимой для принятия обоснованного решения. При недостатке времени часть информации не учитывается, что по последствиям аналогично дефициту информации. Поэтому руководитель требует от своих помощников представлять ему информацию в обобщенном виде и форме, позволяющих воспринять ее в сжатые сроки.

Учитывая жизненную потребность в информации для любых живых организмов, природа создала механизм, заставляющий их искать информацию в случае ее дефицита. Таким общим механизмом для активизации деятельности живых существ по удовлетворению основных потребностей, в том числе информационной потребности, являются эмоции. Уровень отрицательных эмоций живого существа пропорционален дефициту информации, необходимой для принятия им решений. Алгоритм поведения живого человека формируется таким, чтобы устранить причины отрицательных эмоций, в том числе путем поиска информации.

4. **Полезность (цена) информации изменяется во времени**. Распространение информации и ее использование приводят к из-

менению ее ценности и цены. Характер изменения ценности во времени зависит от вида информации. Для научной информации эта зависимость часто имеет волнообразный вид. Информация об открытии даже новых законов или явлений природы вначале должным образом не оценивается. Например, в начале века результаты исследований по атомной физике носили чисто познавательный характер и интересовали узкий круг ученых. Информация в этой области приобрела чрезвычайно высокую цену, когда появились реальные возможности практического использования атомной энергии. По мере того как исчерпываются на определенном этапе научно-технического прогресса возможности практической реализации теоретических результатов, ценность информации убывает. Новые технологии или достижения в смежных областях могут увеличить ценность давно полученных знаний. Недаром говорят, что новое — это хорошо забытое старое.

Ценность (цена) большинства видов информации, циркулирующей в обществе, со временем уменьшается — информация стареет. Характер старения разведывательной информации рассмотрен в [9]. Он приведен на рис. 3.8.




A — оперативно-тактическая информация (ценность теряется 10% в день);
B — стратегическая информация во время войны (ценность теряется 10% в месяц);
C — стратегическая информация в мирное время (ценность теряется 20% в год);
D — информация о сравнительно неизменных объектах (дорогах, мостах, природных ресурсах, ценность теряется 10% в год).

*Рис. 3.8.* Характер старения разведывательной информации

По степени старения коммерческая информация может характеризоваться следующим образом:

- оперативно-тактическая, теряющая ценность примерно по 10% в день (например, информация о выдаче краткосрочного кредита, предложения по приобретению товара в срок до одного месяца и др.);
- стратегическая информация, ценность которой убывает примерно 10% в месяц (сведения о партнерах, о долгосрочном кредите, развитии и т. д.).

Ценность информация о законах природы убывает очень медленно. Ее старение проявляется в уточнении законов, например, в ограничениях законов Ньютона для микромира.

Характер старения информации можно аппроксимировать зависимостью, аналогичной правилу получения «сложного» процента. В соответствии с ней ценность информации через m интервалов времени, убывающая на k процентов за один интервал, оценивается по выражению: $C_и \approx C_{ио}(1 - k/100)^m$, где $C_{ио}$ — ценность информации в момент ее получения. Например, если ценность информации уменьшается в месяц на 10%, то через 6 месяцев она составит около 50% первоначальной ценности. Время, в течение которого ценность информации уменьшается до 10% первоначальной величины, можно назвать **временем жизни информации** $\tau_{жи}$. Время жизни рассматриваемой в примере информации составляет около 21 месяца.

5. **Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации.** Для обеспечения эффективной защиты информации важно знать количество защищаемой информации. Однако объективно определить ее невозможно. Например, количество информации, содержащейся в книге, для разных читателей — разное. Даже один и тот же человек в разные периоды своей жизни находит в книге каждый раз что-то новое для себя. Количество информации в голове человека можно косвенно оценить по его действиям, так как для принятия обоснованного решения необходимо больше информации.

Иногда полезность информации связывают с ее качеством. Но понятие «качество» применительно к информации не имеет само-

стоятельного значения, так как оно поглощается понятием «количество». Действительно, количество информации, например, в фотографии зависит от ее качества. Чем более резкое изображение на фотографии, чем больше в нем полутонов и оттенков цвета, тем больше информации она содержит. Ухудшение качества изображения при копировании, например, видеокассет приводит к снижению количества информации и, как следствие, к уменьшению психологического воздействия фильма на зрителя. Под качеством информации обычно подразумевают качество отображения ее на носителе или ее достоверность (соответствие оригиналу). Качество информации в этом смысле можно достаточно объективно измерить.

Для определения количества информации в теории информации рассматривается так называемый **энтропийный подход**. В соответствии с ним количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество получаемой информации тем больше, чем меньше вероятность события. Такой подход хорошо разработан для определения количества информации в сообщении, передаваемом по каналам связи. Выбор при приеме осуществляется между символами алфавита сообщения. Количество информации в передаваемом по каналам связи сообщении из N символов (без учета связи между символами в сообщении) рассчитывается по известной формуле Шеннона:

$$I = N \sum_{i=1}^{n} P_i \log_2 P_i,$$

где $P_i$ — вероятность появления в сообщении символа i; n — количество символов в алфавите языка.

Как следует из формулы, количество информации, измеряемое в двоичных элементах (в битах, байтах), зависит только от количества и статистики символов, но не зависит от содержания сообщения. Количество информации, определяемое по этой формуле, одинаковое при передаче бессмысленного текста или сообщения о жизненно важных для получателя сведениях, содержащих одинаковые символы. С точки зрения передачи таких сообщений по каналам связи такой подход обоснован, так как затраты на передачу этих сообщений одинаковы. А на что потрачены деньги отправи-

теля сообщения и насколько оно информативно для получателя, — эти вопросы к связи отношения не имеют.

Аналогично, когда при телефонном разговоре ваш собеседник сообщает известные сведения, то количество полученной вами информации мало, хотя разговор может длиться достаточно долго. В таком случае возникает вопрос, что передавалось в этом случае. Очевидно, что осуществлялась передача лишь акустических и электрических сигналов.

Если информацию трактовать как знания, то количество информации, извлекаемой человеком из сообщения, можно оценить степенью изменения его знаний. Структурированные знания, представленные в виде понятий и отношений между ними, называются **тезаурусом**. Тезаурус имеет иерархическую структуру. Понятия и отношения, группируясь, образуют другие, более сложные понятия и отношения.

Знания отдельного человека, организации, государства образуют соответствующие тезаурусы. Тезаурусы различных организационных структур включают части тезаурусов входящих в их состав элементов, прежде всего людей. Например, тезаурус организации образуется из тезаурусов сотрудников по тематике их работы и других носителей информации (документов, продукции, материалов и т. д.).

Для передачи знаний тезаурусы должны пересекаться, т. е. они должны содержать общие элементы (понятия и отношения между ними). Если таковых нет, то владельцы разных тезаурусов просто не поймут друг друга. О таких людях говорят, что они разговаривают на «разных языках». Даже люди одной национальности часто говорят на «разных языках», вкладывая в одинаковые по форме понятия разное содержание. Подход к оценке количества информации по степени изменения тезауруса после ее получения, предложенный Ю. А. Шрейдером, можно назвать **тезаурусным**.

В общем случае количество информации, получаемое из сообщения ее получателем, зависит от соотношения тезауруса сообщения и получателя. Если тезаурус сообщения составляет часть тезауруса получателя или их тезаурусы настолько отличаются по составу, что не пересекаются, то количество получаемой информации минимальное. В первом варианте получатель не при-

обретает новые знания и тезаурус получателя не пополняется, во втором — получатель не понимает смысл сообщения и не может установить отношения с другими элементами тезауруса. Подобное происходит, когда совершаются «преждевременные» научные открытия, которые даже для научной общественности являются «вещью в себе». В истории науки и искусства много фактов отторжения общественностью идей и произведений, опережающих «свое время». Например, доклад русского математика Н. И. Лобачевского на заседании физико-математического факультета Казанского университета в 1826 г. с изложением основ созданной им неевклидовой геометрии, которые рассматриваются в настоящее время как крупнейшее достижение математической мысли в истории мировой науки, почти никем не был понят и подвергся резкой критике.

Обобщая сказанное, циркуляцию информации в человеческом обществе можно представить исходя из следующей модели.

Тезаурусы человека и любой организационной структуры представляют их капитал. Поэтому они стремятся, во-первых, к сохранению (безопасности) своего тезауруса, а во-вторых, к его увеличению. Тезаурус владельца информации может быть увеличен как за счет синтеза знаний владельцем путем проведения собственных исследований или разработок, так и за счет их законного и незаконного приобретения.

Законное приобретение знаний возможно путем организованного обучения в учебных заведениях, самостоятельного изучения литературы (самообучения), приглашения на работу более знающего специалиста, покупки патента или лицензии. Приобретение знаний путем хищения информации является незаконным способом увеличения тезауруса.

Приближенно относительное количество информации можно оценить путем определения доли тематических вопросов, на которые получены ответы, удовлетворяющие потребителя или получателя информации. С этой целью вся предметная область, которая интересует получателя информации, разделяется на n тематических вопросов, из которых на m получены ответы с достаточной полнотой и достоверностью, а отношение n/m характеризует в долях или процентах количество информации. Чем большее количество тематических вопросов, тем точнее оценки.

Применительно к видам информации количества информации приближенно можно оценить на основе следующих соображений.

Учитывая, что любая информация содержится в значениях признаков ее носителя, информацию можно разделить на отдельные минимальные порции, каждая из которых содержит информацию об одном признаке. Наибольшее количество информации содержится в именном признаке с информативностью 1. Информацию о таком гипотетическом признаке можно принять за первичный (базовый) **элемент признаковой информации (ЭПИ)**. Все реальные признаки с информативностью менее 1 составляют долю элемента информации, равную их информативности. Такой же подход можно распространить на количество информации, содержащейся в признаковой структуре. Информация о признаковой структуре в единицах признаковой информации равна ее информативности, которая определяется исходя из информативности составляющих ее признаков по формуле сложения вероятностей. Следовательно, увеличение количества признаковой информации можно обеспечить за счет повышения как информативности признаков, так и их количества.

В качестве единицы семантической информации по аналогии с признаковой информацией целесообразно выбрать то, что пытаются выделить в любом документе, — **мысль**. Она может быть выражена одним словом или большим количеством предложений. Но семантическая информация нужна человеку для передачи прежде всего мыслей. Цена информации также зависит от полезности и количества содержащихся в них мыслей. Формальным путем выявить мысль пока нельзя. Однако человек может в любом сообщении определить, по крайней мере, основные из содержащихся в нем мыслей. Мысли реферата, доклада, курсовой работы, дипломного проекта и других документов концентрируют в заключении. Конечно, сами мысли могут существенно отличаться по ценности или полезности. За одни мысли ее автор получает Нобелевскую премию, другие мысли не интересны даже близкому человеку. Если ценность мысли оценить коэффициентом в интервале 0–1, то количество семантической информации в сообщении определяется как взвешенная (по ценности) сумма содержащихся в нем мыслей.

Такой подход хорошо согласуется с широко применяемой оценкой информации в выступлениях, статьях, отчетах и других информационных материалах. Например, в выступлении такого-то докладчика много полезных мыслей, в статье такого-то автора не содержится ни одной стоящей мысли. Полезность публикации соответственно содержащихся в ней мыслей определяется по количеству ссылок на нее в работах других авторов. Чем более кратко и четко излагает человек свои мысли, тем больше он ценится как специалист.

На практике используют более грубый и простой, так называемый **объемный способ измерения информации** путем подсчета количества (в битах или байтах) символов сообщения или измерения характеристик носителя (количества листов, времени передачи сообщения и др.). Часто покупатели книг оценивают их полезность по количеству листов. Интуитивно кажется, что большее число листов содержит большее количество информации. Но такая зависимость верна далеко не всегда. Сравнительно небольшой по объему рассказ Э. Хемингуэя «Старик и море» превосходит по эмоциональному воздействию многие толстые романы.

6. **Информация способна случайным образом «растекаться» в пространстве**. Так как человеку присуща любознательность, переходящая у многих в любопытство, а также иногда даже трудно сдерживаемое желание поделиться с другими новостями, то при общении (взаимодействии) людей происходит выравнивание их тезаурусов. Следовательно, в организации и обществе, если не предпринимаются дополнительные усилия по поддержанию неравномерности информационной энтропии, происходит ее выравнивание, т. е. выравнивание тезаурусов разных сотрудников или членов общества. Выравнивание тезаурусов происходит путем передачи информации от тезауруса большего объема тезаурусу меньшего объема. Кроме целенаправленной (законной или незаконной) деятельности по передаче информации имеют место случайные процессы выравнивания тезаурусов владельцев, аналогично выравниванию температуры в замкнутом пространстве. Этот процесс объективно проявляется в любой организации, государстве и человеческом обществе в целом путем случайных, трудно контролируемых процессов распространения

информации от источника с большим объемом тезауруса к получателю, в том числе несанкционированному, с меньшим объемом тезауруса. Как показывает опыт, со временем круг лиц, которым становится известна секретная (конфиденциальная) информация, расширяется случайным образом. Кто-то под большим секретом рассказал новости приятелю или жене, те приоткрыли тайну другим людям и т. д. Это процесс объективный в том смысле, что только за счет дополнительных усилий и часто больших затрат удается приостановить или замедлить процесс «растекания» информации. По своей сути он аналогичен, только в информационной сфере, процессу выравнивания энтропии в природе. Например, при уменьшении энтропии в какой-либо точке пространства, вызванном нагреванием или даже рождением человека, со временем температура выравнивается, а человек умирает и превращается в прах, энтропия которого неизмеримо выше, чем у живого человека.

При выравнивании тезаурусов коммерческая цена информации убывает, а ценность информации может как возрастать, так и снижаться. Действительно, закон Ома знают очень много людей, но от этого полезность его для практики не уменьшается. Но покупателя на эту информацию вряд ли удастся найти, так как изучение закона Ома входит в программу школьного образования.

7. **При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается**. После снятия копии с документа на ксероксе или другим способом количество информации в нем не меняется. В результате этого несанкционированное копирование (хищение) информации может остаться незамеченным для ее владельца, если отсутствуют иные признаки проникновения злоумышленника к ее источнику и факта хищения. Но если при копировании происходят воздействия на информационные параметры носителя, приводящие к изменению их значений, или незначительные изменения накапливаются, то количество информации уменьшается. Ухудшается качество звука и изображения соответственно на аудио- и видеопленке из-за механического разрушения магнитного слоя, книжка зачитывается до дыр, блекнут яркие цвета на картинках-репродукциях на стенах светлой комнаты.

Так как при каждом копировании увеличивается число ее законных и незаконных пользователей, то в соответствии с законами рынка цена снижается. Например, видеопиратство вызывает большое беспокойство у владельцев видеопродукции, так как широкое распространение пиратских копий значительно сбивает цены на рынке.

## 3.5. Носители и источники информации

Широко применяемое понятие «носитель информации» имеет разнообразный смысл. Например, человек как носитель информации, учебник, магнитный или бумажный носитель, магнитное поле, электрический ток и др. Эти термины отличаются уровнем конкретизации этого понятия. **Материальные объекты являются носителями признаковой информации на физическом уровне ее представления**. Она содержится в значениях признаков объектов. Носители признаковой информации целесообразно обозначить как первичные. Такими носителями являются:

- макротела;
- поля;
- микрочастицы (элементарные частицы).

**Макротела** являются наиболее долговременными носителями различных видов информации. Прежде всего, материальные тела содержат информацию о своем составе, структуре (строении), о воздействии на них других материальных тел. Например, по остаточным изменениям структуры бумаги восстанавливают подчищенные надписи, по изменению структуры металла двигателя определяют его заводской номер, перебитый автомобильными ворами. Материальные тела (папирус, глиняные таблички, береста, камень, бумага) использовались людьми для консервации и хранения информации в течение всей истории человечества. И в настоящее время бумага является самым распространенным носителем семантической информации. Однако четко прослеживается тенденция замены бумаги машинными носителями (магнитными, полупроводниковыми, светочувствительными и др.), но бумага еще длительное время останется наиболее массовым и удобным носителем, прежде всего, семантической информации.

Носителями информации являются также различные **поля**. Из известных полей в качестве носителей применяются акустические, электрические, магнитные и электромагнитные (в диапазоне видимого и инфракрасного света, в радиодиапазоне). Информация содержится в значениях параметров полей. Если поля представляют собой волны, то информация содержится в их амплитуде, частоте и фазе.

Из многочисленных **элементарных частиц** в качестве носителей информации используются электроны, образующие статические заряды и электрический ток, а также частицы (электроны и ядра гелия) радиоактивных излучений. Попытки использования для переноса информации другие элементарные частицы с лучшей проникающей способностью (меньшим затуханием в среде распространения), например, нейтрино, не привели пока к положительным результатам.

В качестве носителей информации часто рассматривают также материальные тела, содержащие первичные носители. Например, человек как носитель информации содержит разнообразные первичные носители информации в виде химических веществ, электрических сигналов и полей. Человек как носитель информации ее запоминает и пересказывает получателю в письменном виде или устно. При этом он может полученную от источника информацию преобразовать в соответствии с собственным толкованием ее содержания, исказив смысл. Кроме того, человек может быть также носителем других носителей информации — документов, продукции и т. д. Также машинный носитель информации (гибкий или жесткий диск, магнитная лента) представляет собой вторичный носитель по отношению к магнитному полю ферромагнитного слоя на его поверхности. Поэтому такие носители являются **вторичными**.

Носители информации в виде физического процесса или явления называются также **сигналом** — радиосигналом, акустическим сигналом и т. д. В радиотехнике под сигналом подразумевается физическое явление или процесс, несущие информацию.

**Источниками информации** являются субъекты и объекты, от которых может быть получена информация. Все материальные объекты (тела, микрочастицы и поля) являются источниками пер-

вичной признаковой информации, содержащейся в значениях видовых, сигнальных и вещественных признаках. Если эти значения соответствуют также семантической информации, то материальные объекты являются одновременно носителями — переносчиками семантической информации.

Что касается источников семантической информации, то далеко не все объекты и субъекты являются ее источниками. Следует различать прямые и косвенные источники семантической информации. **Прямыми источниками семантической информации** являются ее первичные источники, т. е. отдельные люди или группы людей, являющиеся создателями информации, документы, в которых эта информация отображается. Критерием отнесения носителя семантической информации к ее источнику является возможность оценки достоверности информации, содержащейся на носителе. Это условие для источника семантической информации исключает из их числа технические средства сбора, обработки, хранения и передачи информации, а также людей, транслирующих информацию. Например, телефонный аппарат не может быть источником речевой информации, так как он является лишь техническим средством ее передачи. При анализе достоверности полученной по телефону информации ссылаются не на телефонный аппарат, а на абонента. Также диктор радио и телевидения, зачитывающий текст перед микрофоном или телекамерой, не является источником информации и не несет ответственности за озвученное сообщение. При передаче через СМИ непроверенной оперативной информации сотрудники редакции во избежание привлечения их к судебной или иной ответственности ссылаются на источники этой информации (организации или конкретных людей).

**Косвенными** источниками семантической информации могут быть, в принципе, любые объекты: продукция, материалы, технологическое оборудование, отходы производства и т. д. Например, специалист по видовым, сигнальным и вещественным признакам новой продукции может определить ее технические характеристики.

Информативность **людей** как источников семантической информации существенно различается. Наиболее информированы руководители организаций, их заместители и ведущие специ-

алисты. Каждый сотрудник организации владеет конфиденциальной информацией в объеме, превышающем, как правило, необходимый для выполнения его функциональных обязанностей. Распространение конфиденциальной информации между сотрудниками организации является одним из проявлений процессов выравнивания тезаурусов. Например, в результате неформальных межличностных отношений (дружественных, приятельских) конфиденциальная информация может поступать к посторонним лицам, которые к сохранению «чужих» тайн относятся менее ответственно, чем к своим. Тщеславные люди с целью продемонстрировать свою эрудицию или заинтересовать собеседника непреднамеренно разглашают конфиденциальные сведения в публичных выступлениях и беседах. Кроме непреднамеренного разглашения конфиденциальной информации часть сотрудников (по американской статистике — около 25%) по различным личным мотивам готовы продать известные им секреты и ищут контактов с зарубежной разведкой или представителями конкурента.

Поэтому служба безопасности в интересах локализации ценной информации должна постоянно помнить о достаточно объективных процессах распространения информации внутри и даже за ее пределами (через родственников, друзей и приятелей, через сотрудников налоговой полиции, муниципалитетов, префектур, в арбитражном суде и т. д.). Даже эффективная защита информации, но только в пределах организации, не гарантирует ее безопасность.

В [2] под **документом** понимается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. К документам относится служебная информация, научные публикации в открытой и закрытой печати, статьи в газетах и журналах о деятельности организации или ее сотрудников, реклама, отчеты сотрудников, конструкторская и технологическая документация и т. д.

**Документы** относятся к наиболее информативным источникам, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде, в особенности если документы подписаны или утверждены. Информативность различных публикаций имеет широкий диапазон оценок: от очень высокой, когда описывается открытие, до преднамеренной или непреднамеренной де-

зинформации. К последней, например, относятся публикации с недостаточно проверенными и достоверными результатами.

Технические средства сбора, обработки, хранения и передачи информации нельзя отнести к источникам семантической информации, так как они представляют собой лишь инструмент для преобразования входной информации.

Часто к источникам семантической информации относят компьютеры. Однако несмотря даже на их впечатляющие возможности, превосходящие по объему и скорости обработки возможности человека, их работа определяется программами, созданными человеком. Можно ли, например, рассматривать компьютер Deep Blue фирмы IBM, с помощью которого удалось выиграть матч по шахматам у чемпиона мира Г. Каспарова, как источник информации? По-видимому, для этого основания нет, так как известные алгоритмы игры компьютера в шахматы основаны на возможности компьютера за счет существенно большего быстродействия просчитывать и оценивать большее число ходов, чем может сделать это шахматист. Но талантливый шахматист способен не только просчитывать несколько ходов вперед, но и интуитивно выбирать ход, который обеспечивает ему в большинстве случаях выигрыш с быстродействующим компьютером. Можно утверждать, что, пока компьютер при обработке информации строго следует программе любой сложности, его нельзя считать источником семантической информации. Следовательно, источником информации, полученной в результате обработки даже очень сложной программы, является автор метода обработки. Компьютер станет источником информации, когда он будет обладать искусственным интеллектом, т. е. способностью к абстрактному мышлению. Работы по созданию таких компьютеров ведутся, однако проблема оказалась существенно сложнее, чем представляли ее создатели искусственного интеллекта как направления кибернстики.

Состав косвенных источников семантической информации существенно больший — измерительные приборы, продукция, оборудование, материалы и т. д.

**Продукция** (без документации) является источником информации о признаках. Ноу-хау нового изделия могут содержаться во внешнем виде, например, в форме автомобиля, расцветке ткани,

моделях одежды, узле механизма, в параметрах излучаемых полей (сигналов радиостанции или радиолокатора), в составе и структуре материала (броневой стали, ракетного топлива, духов или лекарства). Для получения семантической информации о сущности ноу-хау с целью его использования производят изучение и исследование продукции путем разборки, расчленения, выделения отдельных составных частей и элементов, проведения физического и химического анализа и т. д.

Любой творческий и производственный процесс сопровождается **отходами**. Редкие люди способны формулировать свои мысли в окончательном варианте, без черновиков с различными вариантами, без коррекции ранее изложенного. Научные работники создают макеты будущих изделий или пробы веществ, при производстве (опытном или промышленном) возможен брак или технологические газообразные, жидкие или твердые отходы. Даже при печатании на пишущей машинке остаются следы документов на копировальной бумаге и ленте, которые после использования неопытная или небдительная машинистка бросает в корзину для бумаг. Отходы производства в случае небрежного отношения с ними (сбрасывания на свалку без предварительной селекции, сжигания или резки бумаги и т. д.) могут привести к утечке ценной информации. Для такой возможности существуют, кроме того, психологические предпосылки сотрудников, серьезно не воспринимающих отходы как источники секретной (конфиденциальной) информации.

Информативными могут быть не только продукция и отходы ее производства, но и исходные **материалы и сырье**, а также используемое **оборудование**. Если среди поставляемых фирме материалов и сырья появляются новые наименования, то специалисты конкурента могут определить по ним изменения в создаваемой продукции или технологических процессах.

Важнейшими показателями источника информации являются его **информативность** и **надежность**. Информативность источника информации оценивается полнотой ответов с помощью полученной от него информации на поставленные перед органом добывания вопросы. Если информация источника позволяет ответить на m из n поставленных вопросов, то информативность ис-

точника оценивается как $I_{ни} = m/n$. Надежность источника характеризуется достоверностью получаемой от источника информации. Достоверность информации очень надежного источника близка к 1.

Источниками признаковой информации являются материальные объекты и процессы. Они содержат информацию как о собственных признаках, так и признаках, взаимодействующих с ними объектов и процессов.

## 3.6. Запись и съем информации с ее носителя

В редких случаях информация от источника непосредственно передается получателю, т. е. источник сам переносит ее в пространстве к месту расположения получателя или получатель вступает в непосредственный контакт с источником, например проникает в помещение, вскрывает сейф и забирает документ. В большинстве случаев она переносится от источника к получателю промежуточным носителем.

Материализация (запись) любой информации производится путем изменения параметров носителя. Механизм запоминания и воспроизведения информации человеком в настоящее время еще недостаточно изучен и нет однозначного и ясного представления о носителях информации в мозгу человека. Рассматривается химическая и электрическая природа механизмов запоминания.

Запись информации на материальные тела производится путем изменения их физической структуры и химического состава. На бумаге информация записывается путем окрашивания элементов ее поверхности типографской краской, чернилами, пастой и другими красителями.

Записанная на материальном теле информация считывается при просмотре поверхности тела зрительным анализатором человека или автомата, обнаружении и распознавании ими знаков, символов или конфигурации точек. Для людей, лишенных зрения, информация записывается по методу Брайля путем изменения физической структуры бумаги выдавливанием соответствующих знаков (букв и цифр). Информация считывается не зрительным анализатором, а тактильными рецепторами пальцев слепых людей.

Запись информации на носители в виде полей и электрического тока осуществляется путем изменения их параметров. Непрерывное изменение параметров сигналов в соответствии со значениями первичного сигнала называется **модуляцией**, дискретное — **манипуляцией**. Первичным является сигнал от источника информации. Модулируемое колебание называется **несущим**. Если меняются значения амплитуды аналогового сигнала, то модуляция называется амплитудная (АМ), частоты — частотная (ЧМ), фазы — фазовая (ФМ). Максимальное изменение информационного параметра несущей относительно его номинального значения называется **глубиной модуляции**, а максимальное отклонение значения информационного параметра несущей относительно максимального изменения информационного параметра модулирующего сигнала — **индексом модуляции**.

При модуляции дискретных сигналов в качестве признаков применяются также длительность импульса, частота его повторения и др. С целью уплотнения информации на носителе и экономии тем самым энергии носителя применяют сложные (с одновременным использованием различных параметров сигнала) виды модуляции. Например, для радиовещания в УКВ-диапазоне (58–73, 87,5–108 МГц) используется частотная модуляция с максимальным изменением (девиацией) частоты 50 кГц. При максимальной частоте модулирующего сигнала 15 кГц индекс частотной модуляции составляет $\beta_ч = 3{,}3$, а глубина модуляции на частоте 100 МГц — 0,0005.

В соответствии с формулой Фурье изменение формы сигнала при модуляции приводит к изменению спектра модулированного сигнала. Чем выше максимальная частота спектра моделирующего сигнала $F_{с.м}$, тем шире спектр модулированного сигнала. Количественное значение увеличения ширины спектра этого сигнала зависит от вида модуляции, ширины спектра модулирующего (первичного) сигнала, глубины и индекса модуляции. Ширина спектра модулированного синусоидального сигнала составляет величины [10]:

- для АМ: $\Delta F_{ам} = 2F_{с.м}$;
- для ЧМ: $\Delta F_{чм} >> F_{с.м}$;
- для ФМ: $\Delta F_{фм} \approx \Delta F_{чм}$.

Ширина спектра широко применяемых модулированных сигналов составляет:

- телеграфных сигналов (CW) — около 1 кГц;
- АМ-узкополосных сигналов, используемых в радиовещании на длинных, средних и коротких волнах, — 5–15 кГц;
- используемых для радиосвязи ЧМ-узкополосных (NFM) — 5–15 кГц;
- ЧМ-широкополосных (WFM) в УКВ радиовещании и при передаче звука в телевидении — 150–250 кГц.

Ширина спектра ЧМ-сигнала составляет 50–250 кГц вместо 7 кГц для АМ речевого сигнала. Поэтому ЧМ-сигналы не применяют из-за «тесноты» в эфире в длинноволновом, средневолновом и даже коротковолновом диапазонах волн. ЧМ-вещание ведется в УКВ-диапазоне. Так как действие помех проявляется, прежде всего, в изменении амплитуды сигнала, то ЧМ-сигналы обладают существенно большей помехоустойчивостью, чем АМ-сигналы. Это свойство ЧМ-сигналов обеспечивает высокое качество радиовещания в УКВ-диапазоне. Спектры ФМ- и ЧМ-сигналов мало отличаются по ширине.

Выделение информации из модулированного электрического сигнала производится путем обратных преобразований — **демодуляции** его в детекторе (демодуляторе) приемника. При демодуляции выделенный и усиленный сигнал, наведенный электромагнитной волной в антенне, преобразуется таким образом, что сигнал на выходе детектора соответствует модулирующему сигналу передатчика. Демодуляция, как любая процедура распознавания, обеспечивается путем идентификации текущей признаковой структуры сигнала с эталонной структурой, заданной априори или полученной в процессе его приема. Эталонная признаковая структура при ЧМ-модуляции определяется частотой настройки контура детектора. При демодуляции АМ-сигналов в качестве эталонной амплитуды используется усредненная амплитуда несущего колебания на выходе детектора, относительно которой сравнивается текущее значение амплитуды принимаемого сигнала. Для демодуляции ФМ-сигнала необходимо знать значение фазы несущего колебания до его модуляции.

Из-за влияния помех модулирующие (при передаче) и демодулированные (при приеме) сигналы будут отличаться. В общем случае любые преобразования сигнала с воздействием на его информационные параметры изменяют записанную в нем информацию. Степень изменения зависит от отношения сигнал/помеха на входе демодулятора. При достаточно большом превышении мощности носителя над мощностью помех искажения информации столь незначительные, что количество и качество информации практически не меняются.

Помехоустойчивость дискретных сигналов выше, чем аналоговых, так как искажения дискретных сигналов возникают в тех случаях, когда изменения параметра сигнала превышают половину величины интервала между соседними значениями параметра. Если изменения параметров помехами составляют менее половины этого интервала, то при приеме такого сигнала можно восстановить исходное значение параметра сигнала. Допустимые значения отношения мощностей или амплитуд сигнала и помехи (отношения сигнал/помеха), при которых обеспечивается требуемое качество принимаемой информации, определяются видом информации и характером помех.

Для повышения достоверности передачи информации наряду с увеличением энергии носителя информации используют другие методы защиты дискретной информации от помех, прежде всего помехоустойчивое кодирование. При помехоустойчивом кодировании каждому элементу дискретной информации (букве, цифре, любому другому знаку) ставится в соответствие кодовая комбинация, содержащая дополнительные (избыточные) двоичные символы. Эти дополнительные символы позволяют обнаруживать искажения и исправлять в зависимости от избыточности кода ошибочные символы различной кратности. Существует большое количество видов кодов, повышающих помехоустойчивость сообщений для различных условий среды распространения носителей. Однако следует иметь в виду, что платой за повышение помехоустойчивости кодированных сигналов является уменьшение скорости передачи информации.

Любое сообщение в общем случае можно описать с помощью трех основных параметров: динамического диапазона $D_c$, шири-

ны спектра частот $\Delta F_c$ и длительности передачи $T_c$. Произведение этих трех параметров $V_c = D_c \Delta F_c T_c$ называется **объемом сигнала**. В трехмерном пространстве объем сигнала можно представить в виде параллелепипеда (см. рис. 3.9).

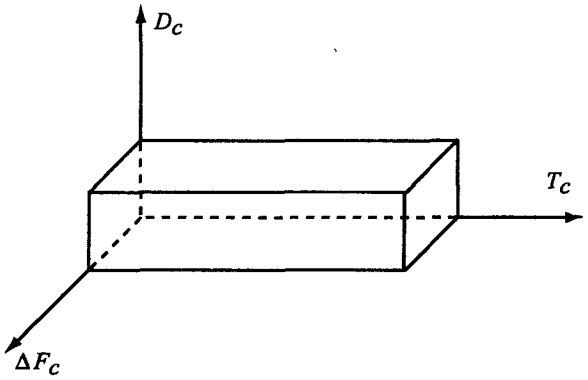



*Рис. 3.9.* Графическое представление объема сигнала

Для обеспечения неискаженной передачи сообщения объемом $V_c$ необходимо, чтобы характеристики среды распространения и непосредственно приемника соответствовали ширине спектра и динамическому диапазону сигнала.

Если полоса частот среды распространения или приемника уже полосы сигнала, то для обеспечения безыскаженной передачи сигнала объемом $V_c$ уменьшают его ширину спектра. При этом для сохранения $V_c = \text{const}$ соответственно увеличивают время передачи $T_c$. Для безыскаженной передачи сообщения в реальном масштабе времени полоса пропускания приемника должна соответствовать ширине спектра сигнала.

### Вопросы для самопроверки

1. Сущность признакового подхода к информации.
2. Что представляет собой язык признаков?
3. Чем первичные источники информации отличаются от вторичных?
4. Чем отличаются источники признаковой информации от источников семантической информации?
5. Источником какого вида информации является компьютер?

6. Для чего создаются профессиональные языки? Отличия языков национального общения от профессиональных.
7. Математическая интерпретация информативности признака.
8. Отличия признаков аналоговых и дискретных сигналов.
9. Отличие ценности информации от ее цены. Составляющие цены информации.
10. Стареют ли исторические документы?
11. Почему нельзя объективно измерить количество информации? Чем измеряют количество информации?
12. Почему говорят, что если тайна известна более чем одному человеку, она известна всем?
13. Первичные и вторичные носители информации. К какому носителю информации относится человек?
14. Почему телефонный аппарат нельзя рассматривать как источник семантической информации? Какими качествами должен обладать источник семантической информации?
15. Чем отличаются прямые и косвенные источники информации?
16. Виды модуляции гармонического колебания.
17. Что надо знать для демодуляции сигнала?

# Глава 4. Характеристика угроз безопасности информации

## 4.1. Виды угроз безопасности информации

Угрозы создают потенциальную опасность для объекта или предмета защиты. Сосулька на крыше дома весной создает угрозу жизни прохожих, но она не влияет на их здоровье, пока не упадет на голову. Также изменения в информации или ее хищение возникают при реализации угроз. Следовательно, **угрозы представляют собой состояния или действия взаимодействующих с носителями информации субъектов и объектов материального мира, которые могут привести к изменению, уничтожению, хищению и блокированию информации**. Под блокированием информации понимаются изменения условий хранения информации, которые делают ее недоступной для пользователя. По виду реализации угрозы можно разделить на две группы:

- физическое воздействие внешних сил на источники информации, в результате которого возможны ее изменения, уничтожение, хищение и блокирование;
- несанкционированное распространение носителя с защищаемой информацией от ее источника до злоумышленника, которое приводит к хищению информации.

Угрозы, при реализации которых происходит воздействие различных сил (механических, электрических, магнитных) на источник информации, называются **угрозами воздействия на источник информации**, а угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику, — **угрозами утечки информации**. Классификация угроз рассмотрена на рис. 4.1.

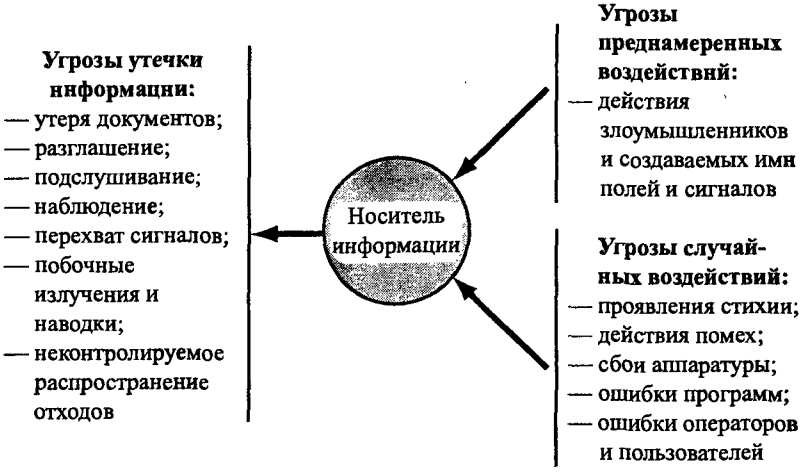



*Рис. 4.1.* Виды угроз

Воздействия, которые создаются злоумышленниками, являются **преднамеренными**. К ним относятся как непосредственные воздействия людей (злоумышленников) на источник информации, так и воздействия полей и электрических сигналов технических средств, создаваемых людьми с целью уничтожения, изменения или хищения информации. Например, электромагнитный импульс, возникающий во время атомного взрыва или излучения электромагнитной пушки, способен уничтожить (стереть) информацию на машинных носителях.

На источники информации постоянно действуют случайные силы, вызванные стихией природы, случайными физическими процессами в средствах хранения, обработки и передачи информации, ошибками операторов и технического персонала. Такие угрозы воздействия называются **случайными**. С целью уменьшения влияния неблагоприятных факторов окружающей среды в хранилищах архивов и музеев поддерживают определенную температуру, влажность, химический состав воздуха.

Иногда преднамеренные воздействия называют **несанкционированными воздействиями**, а случайные — **непреднамеренными воздействиями**. Такие определения недостаточно корректные, так как непреднамеренные воздействия могут быть как санкционируемыми, так и несанкционируемыми. Например, студенты

при проведении лабораторных работ любят нажимать кнопки или крутить ручки приборов в лаборатории, несмотря на строгие предупреждения преподавателей. Любопытство людей создало даже дополнительную задачу перед разработчиком радиоэлектронных средств и электрических приборов, которая формулируется как «защита от дурака». Для обеспечения такой защиты кнопки, нажатие на которые может вызвать серьезные изменения в режимах работы средств, защищаются различными экранами, предупредительными надписями или требованиями подтверждения действия, как предусмотрено это в компьютерах при стирании файлов.

Внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести к ее хищению, при распространении от источника внешней силы (внешнего воздействия) до источника информации образуют **канал несанкционированного доступа**. Если эти силы целенаправленно организуются, то канал несанкционированного доступа называется **преднамеренный**, если силы случайные, то канал несанкционированного доступа — **случайный**.

Преднамеренный канал несанкционированного доступа организуется или создается злоумышленником. Когда он пытается проникнуть к месту хранения источника информации, то выбирает путь движения, удовлетворяющий требованиям минимизации риска быть обнаруженным и задержанным, минимизации времени движения злоумышленника. Вектор движения стихийных сил, например природы, к источнику информации определяется физическими условиями окружающей среды и приводит к образованию случайного канала несанкционированного доступа. Причин возникновения каналов несанкционированного доступа очень много. Типовыми из них являются:

- выполнение операции по добыванию информации органом разведки зарубежного государства, конкурента, криминальной структуры;
- попытки несанкционированного получения информации сотрудником организации или иным физическим лицом с целью ее продажи, шантажа, мести и другим мотивам;
- проявление стихийных сил (пожара, наводнения, урагана, землетрясения);

- неисправности программно-аппаратных средств хранения, обработки и передачи информации;
- ошибки в работе с программно-аппаратными средствами операторов и пользователей.

Несанкционированное распространение носителя с информацией от ее источника к злоумышленнику называется **утечкой информации**. Она может возникнуть в результате:

- утери источника информации (документа, продукции и др.);
- разглашения сведений;
- подслушивания;
- наблюдения;
- перехвата электромагнитных полей и электрических сигналов, содержащих защищаемую информацию;
- сбора отходов дело- и промышленного производства.

Эти действия пользователя информации и злоумышленника создают угрозы утечки информации, которые в случае попадания ее к злоумышленнику приводят к утечке.

При **случайной утере** источника закрытой информации они попадут к злоумышленнику при совпадении многих условий, в том числе если источник будет найден злоумышленником или человеком, который ему его передаст. Вероятность этого невысока. Чаще найденный на территории организации источник возвращается человеку, который его потерял, или передается соответствующим должностным лицам.

Утечка информации в результате ее **непреднамеренного разглашения** происходит чаще, чем утеря источника. Даже прошедшие инструктаж люди не могут постоянно контролировать свою речь, особенно в случае повышенного эмоционального состояния. Например, в перерыве закрытого совещания его участники часто продолжают обсуждение вопросов совещания в коридоре и в местах для курения, в которых могут находиться посторонние люди. Разглашение возможно в городском транспорте, на улице, дома, на различных научных и иных конференциях. Ученые для получения признания у зарубежных коллег разглашают полученные научные сведения, содержащие государственную тайну. Они для оправдания своих действий навязывают обществу мнение, что научные результаты принадлежат всему человечеству, забывая при этом, что

человечество состоит из отдельных государств и людей, которые беззастенчиво используют их для достижения собственных целей, противоречащих интересам большинства людей. Слова об общечеловеческих ценностях или интересах народа часто используются как красивые бумажки, в которые заворачивают корысть. История знает много примеров того, к каким бедам и трагедиям людей приводила «борьба за народные интересы и общечеловеческие ценности».

Несанкционированный прием злоумышленником (его техническим средством) сигнала с защищаемой информацией и его демодуляция позволяют ему добывать эту информацию. При этом на носитель никакого воздействия не оказывается, что обеспечивает скрытность добывания. Прием оптических и иных сигналов от объектов и получение с их помощью изображений этих объектов называются **наблюдением**, прием и анализ акустических сигналов — **подслушиванием**, а прием и анализ радио- и электрических сигналов — **перехватом**. Исторически сложившиеся названия могут вызывать неоднозначность толкования. Например, подслушивание может быть непосредственным (с помощью ушей) и с помощью технических средств. Причем в последнем варианте оно может осуществляться в принципе на любом расстоянии, например, путем перехвата междугородних или международных телефонных разговоров.

**Подслушивание** — один из наиболее древних методов добывания информации. Подслушивание, как и наблюдение, бывает непосредственное и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов разговаривающих людей и значительного затухания акустической волны в среде распространения непосредственное подслушивание возможно на небольшом расстоянии (единицы или, в лучшем случае, при отсутствии посторонних звуков — десятки метров). Поэтому для подслушивания применяются различные технические средства. Этим способом добывается в основном семантическая (речевая) информации, а также демаскирующие признаки сигналов от работающих механизмов, машин и других источников звуков.

**Наблюдение** предполагает получение и анализ изображения объекта наблюдения (документа, человека, предмета, пространства и др.). При наблюдении добываются, в основном, видовые признаки объектов. Но возможно добывание семантической информации, если объект наблюдения представляет собой документ, схему, чертеж т. д. Например, текст или схема конструкции прибора на столе руководителя или специалиста могут быть подсмотрены в ходе их посещения. Также возможно наблюдение через окно помещения текста и рисунков на плакатах, развешанных на стене во время проведения совещания.

Объекты могут наблюдаться непосредственно — глазами или с помощью технических средств. Различают следующие способы наблюдения с использованием технических средств:

- визуально-оптическое;
- с помощью приборов наблюдения в ИК-диапазоне;
- наблюдение с консервацией изображения (фото- и киносъемка);
- телевизионное наблюдение, в том числе с записью изображения;
- лазерное наблюдение;
- радиолокационное наблюдение;
- радиотеплолокационное наблюдение.

**Визуально-оптическое наблюдение** — наиболее древний способ наблюдения со времени изобретения линзы. Современный состав приборов визуально-оптического наблюдения разнообразен — от специальных телескопов до эндоскопов, обеспечивающих наблюдение скрытых объектов через маленькие отверстия или щели.

Так как человеческий глаз не чувствителен к ИК-лучам, то для наблюдения в ИК-диапазоне применяются специальные приборы (ночного видения, тепловизоры), преобразующие невидимое изображение в видимое.

Основной недостаток визуально-оптического наблюдения в видимом и ИК-диапазонах — невозможность сохранения изображения для последующего анализа специалистами. Для консервации (сохранения) статического изображения объекта его фотогра-

фируют, для консервации подвижных объектов производят кино- или видеосъемку.

Наблюдение объектов с одновременной передачей изображений на любое, в принципе, расстояние осуществляется с помощью средств **телевизионного наблюдения**.

Возможно так называемое лазерное наблюдение в видимом и ИК-диапазонах, в том числе с определением с высокой точностью расстояния до объекта и его координат.

**Радиолокационное наблюдение** позволяет получать изображение удаленного объекта в радиодиапазоне в любое время суток и в неблагоприятных климатических условиях, когда невозможны другие способы наблюдения. При **радиотеплолокационном наблюдении** изображение объекта соответствует распределению температуры на его поверхности

**Перехват** предполагает несанкционированный прием радио- и электрических сигналов и извлечение из них семантической информации, демаскирующих признаков сигналов и формирование изображений объектов при перехвате телевизионных или факсимильных сигналов.

Многообразие технических средств и их комплексное применение для добывания информации порой размывают границы между рассмотренными способами. Например, при перехвате радиосигналов сотовой системы телефонной связи возможно подслушивание ведущихся между абонентами разговоров, т. е. одновременно производится и перехват и подслушивание. Учитывая неоднозначность понятий «подслушивание» и «перехват», способы добывания акустической информации целесообразно относить к подслушиванию, а несанкционированный прием радио- и электрических сигналов — к перехвату

Следовательно, угрозы утечки информации представляют собой условия и действия, при которых носитель с защищаемой информацией может попасть к злоумышленнику. Угроза утечки информации реализуется, если она попадает к злоумышленнику. Если по тем или иным причинам это не происходит, то угроза не реализуется. Например, утеря документа далеко не всегда приводит к утечке содержащейся в нем документов. Этот документ может про-

лежать в месте его случайного попадания сколь угодно долго или прийти в негодность под действием, например, природных факторов.

Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется **каналом утечки информации**. Если распространение информации производится с помощью технических средств, то канал утечки информации называется **техническим каналом утечки информации**.

Угрозы утечки, так же как угрозы воздействия, могут быть случайными и преднамеренно создаваемыми злоумышленником. Если характеристики источников опасных сигналов злоумышленнику априори не известны, то технические каналы утечки информации являются **случайными**. Когда технический канал утечки информации организуется злоумышленником, например, с помощью закладного устройства, то такой канал утечки информации является **организованным**.

Угроза оценивается по величине ущерба, который возникает при ее реализации. Различается **потенциальный и реальный ущерб**. Потенциальный ущерб существует при появлении угрозы, реальный — при реализации угрозы. Вероятность или риск возникновения угрозы зависит от многих факторов, основными из которых являются:

- цена защищаемой информации;
- уровень защищенности информации;
- квалификация злоумышленника, его ресурс и затраты на добывание им информации;
- криминогенная обстановка в месте нахождения организации.

Чем выше цена информации, тем сильнее побудительный мотив для злоумышленника. Любой здравомыслящий преступник, задумывая преступление, рассчитывает получить больше, чем он потратит на его подготовку и выполнение. Поэтому вероятность угрозы выше 0 тогда, когда цена информации превышает затраты на ее добывание. Она резко возрастает при существенном увеличении отношения цены информации к затратам на ее добывание — $С_и / С_д$. Качественно эта зависимость иллюстрируется кривой на рис. 4.2.

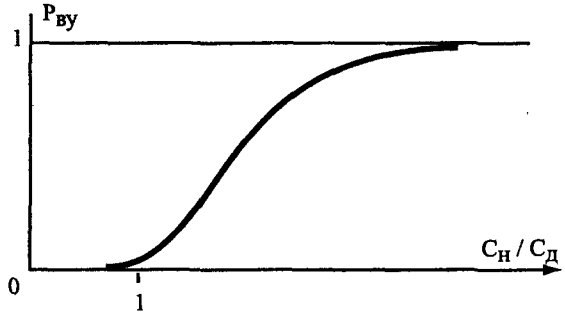



*Рис. 4.2.* Зависимость вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание

Уровень защищенности информации определяет затраты на добывание информации. Его рост уменьшает отношение $C_и / C_д$ и, следовательно, вероятность угрозы.

Как в любой деятельности, эффективность добывания информации зависит от квалификации исполнителя. Чем выше квалификация исполнителя, тем быстрее злоумышленник доберется до источника информации и тем больше вероятность угрозы. Но квалифицированный злоумышленник тщательнее готовится к разведывательной операции и его расходы на нее выше расходов неквалифицированного злоумышленника.

Вероятность возникновения угрозы со стороны криминала зависит также от криминогенной обстановки в районе, городе, объекте федерации и в стране в целом. Там, где криминал чувствует себя хорошо, трудно ожидать, что он не заинтересуется ценной информацией.

Вероятность реализации возникшей угрозы определяется уровнем ее защиты и квалификацией злоумышленника. Чем выше уровень защиты, тем сложнее довести процесс добывания информации до конца.

## 4.2. Источники угроз безопасности информации

Любая угроза, в том числе безопасности информации, имеет свой источник. Эффективно предотвращать угрозы можно, если известны ее источники, так же как нельзя вылечить человека, не

устранив причину болезни, — можно лишь временно устранить ее симптомы. Когда у человека болит голова, он принимает таблетку анальгина или другого болеутоляющего лекарства. Но через некоторое время боль возобновляется. Это будет повторяться до тех пор, пока не будет устранена причина головной боли. Поэтому в современной медицине возрастающее внимание уделяется диагностике болезней, создаются оснащенные современной техникой диагностические центры.

Раскрытие любого преступления начинается также с ответа на вопрос «кому это выгодно?». По этой же причине служба безопасности любой структуры постоянно занимается выявлением источников возможных угроз в деятельности организации или фирмы. Однако сделать это не так просто. Многие источники угроз тщательно маскируются. Между угрозой и ее источником может существовать длинная цепочка посредников. Часто эту цепочку для скрытия источника разрывают, убивая, например, киллера после реализации им угрозы.

Применительно к информации источники угроз можно разделить на группы по видам угроз: **источники угроз воздействий на носитель информации** и **источники угроз утечки информации**. Если деятельность источников угроз направлена на несанкционированное добывание информации, то они являются источниками преднамеренных воздействий. У источников угроз случайных воздействий такая цель отсутствует. Так как целеобразование возможно только у высших животных и у человека, то источниками преднамеренных угроз являются люди, называемые **злоумышленниками**. Их деятельность по добыванию информации может быть индивидуальной или в составе различных государственных, коммерческих или криминальных структур. В общем случае источниками преднамеренных угроз являются:

- органы зарубежной разведки;
- органы разведки коммерческих структур государства;
- криминальные структуры;
- завербованные, психически больные или недовольные своим положением сотрудники организации.

Наибольшие угрозы информации создают профессионалы. Любое государство создает органы разведки, обеспечивающие руководство страны информацией для принятия им политических,

экономических, военных, научно-технических решений в условиях жесткой межгосударственной конкуренции. В зависимости от целей государства, его внешней политики и возможностей структуры органов разведки существенно различаются.

Самую мощную разведку имеют США. В настоящее время, согласно открытой зарубежной печати, структуру разведывательного сообщества США образуют следующие организации:

- Центральное разведывательное управление (ЦРУ);
- Министерство национальной безопасности;
- Разведывательные организации Министерства обороны США;
- Разведывательные подразделения гражданских ведомств США;
- Штаб разведки разведывательного сообщества или Центральная разведка.

ЦРУ является наиболее крупной разведывательной организацией и состоит из пяти основных директоратов (оперативного, научно-технического, информационно-аналитического, административного и планирования) и ряда самостоятельных подразделений (финансово-планового отдела, отдела шифрования, секретариата, управления по связи с общественностью и др.).

Оперативный директорат решает задачи по добыванию информации силами агентурной разведки, организации и проведения тайных операций, по осуществлению контрразведывательного обеспечения агентурной деятельности, по борьбе с терроризмом и наркобизнесом.

Научно-технический директорат проводит исследования и разработки в области технических средств разведки, эксплуатирует стационарные технические комплексы сбора, обработки и передачи информации, обеспечивает сотрудничество с научными центрами США.

Информационно-аналитический директорат проводит обработку и анализ разведывательной информации и готовит выходные документы для президента, Совета национальной безопасности, конгресса и других потребителей.

Административный директорат занимается вопросами подбора кадров на работу в ЦРУ, их подготовкой и переподготовкой, обеспечивает безопасность персонала и объектов ЦРУ и др.

Директорат планирования занимается планированием и координацией деятельности разведки.

В число разведывательных подразделений Министерства обороны входят:

- разведывательные подразделения собственно Министерства обороны;
- разведывательные подразделения Министерства армии США;
- разведывательные подразделения Министерства ВВС США;
- разведывательные подразделения ВМС США.

Основными подразделениями разведки Министерства обороны являются:

- разведывательное управление Министерства обороны (РУМО), занимающегося военно-стратегической разведкой;
- Агентство национальной безопасности (АНБ), которое ведет радиоэлектронную разведку, а также разрабатывает коды и шифры. Оно располагает одним из самых крупных центров по обработке данных, самыми мощными ЭВМ, имеет около 2 тыс. станций радиоэлектронного перехвата, численность персонала составляет более 120 тыс. человек. Силы и средства АНБ составляют основу системы радиоэлектронной разведки «Эшелон», обеспечивающей перехват информации по всему миру;
- Национальное управление военно-космической разведки.

К разведывательным организациям гражданских ведомств США относятся:

- управление разведки и исследований Госдепартамента;
- разведывательные подразделения Министерства энергетики;
- разведывательные подразделения Министерства торговли;
- разведывательные подразделения Министерства финансов;
- управление Федерального бюро расследований (ФБР).

Разведка Госдепартамента обеспечивает сбор информации, необходимой для проведения внешней политики США, участвует в разработке разведывательных операций и национальных разведывательных программ США.

Разведывательные подразделения других ведомств собирают информацию об экспортных операциях, о финансовом и валютном положении иностранных государств, об энергетике других госу-

дарств, особенно об атомной энергетике, разработке и производстве ядерного оружия и по другим вопросам.

Управление контрразведки ФБР не только само ведет сбор разведывательной информации об иностранных гражданах, но и оказывает помощь другим организациям разведывательного сообщества.

Даже из краткого перечня разведывательных служб США следует, что разведкой занимаются все основные государственные структуры: от президента, который возглавляет СНБ, до различных ведомств.

В целях снижения дублирования деятельности многочисленных организаций, собирающих разведывательную информацию в интересах различных ведомств страны, координацию деятельности всех организаций разведывательного сообщества осуществляет штаб центральной разведки, который возглавляет директор ЦРУ.

Разведывательным сообществом развернута разведывательная сеть практически во всех странах мира, разведкой занимаются сотни тысяч штатных сотрудников и привлекаемых специалистов. Финансовые возможности разведывательного сообщества достигают уровней бюджетов развивающихся стран.

Мощную разведку имеют другие развитые страны, прежде всего Россия, Великобритания, Германия, Франция, Израиль.

Состав органов разведки коммерческих структур существенно различается в зависимости от ее возможностей, прежде всего, капитала и вида деятельности. Разведка промышленных гигантов может составить конкуренцию государственной разведке. Разведкой мелкой фирмы могут заниматься всего несколько человек службы безопасности.

Организованная преступность располагает также большими финансовыми и техническими возможностями для ведения разведки и добывания информации.

Преднамеренные угрозы воздействия реализуются путем **непосредственного и дистанционного воздействия** на источник информации. Для непосредственного воздействия на источник информации злоумышленник должен проникнуть к источнику информации, преодолев рубежи защиты и контролируемые зоны. Очевидно, что риск обнаружения и задержания злоумышлен-

ника силами и средствами системы защиты информации велик. Существенно меньший риск для злоумышленника возникает при использовании им средств дистанционного воздействия на информационные параметры источника информации.

Современные средства силового разрушающего воздействия представляют собой по существу электромагнитное оружие, способное дистанционно вывести из строя любую информационную систему, в том числе уничтожить хранящуюся или обрабатываемую в ней информацию. Электромагнитное оружие генерирует поток кратковременных (длительностью в единицы и менее нс) и чрезвычайно мощных электрических (напряжением единицы и десятки кВ) или радиоимпульсов (мощностью в сотни и тысячи кВт), которые, распространяясь по проводам или в пространстве в виде узконаправленного луча, разрушают элементы радиоэлектронных средств обработки и хранения информации и (или) изменяют значения информационных параметров носителей информации.

Органы разведки различных структур являются источниками угроз воздействий и утечки информации. Они могут оказывать как воздействия на источник информации, так и на носители ее в виде сигналов и отходов производства. Источники случайных угроз отличаются от преднамеренных угроз отсутствием у них целей по изменению, уничтожению, хищению и блокированию информации.

Источники угроз случайных воздействий могут быть:

- стихийные силы (пожар, наводнение, ураган, землетрясение и др.) и действия по их нейтрализации;
- пришедшие в негодное состояние инженерные конструкции, цепи электроснабжения, трубы водо- и теплоснабжения и другие элементы инфраструктуры мест установки средств информационного обеспечения;
- технические средства сбора, обработки, передачи и хранения информации, содержащие неисправные элементы;
- программы, содержащие ошибки и вирусы;
- неквалифицированные или плохо выполняющие свои обязанности операторы и персонал, обслуживающий программно-аппаратные средства;
- грызуны и насекомые в местах размещения информационных средств.

Теоретические вопросы противоборства двух сторон рассматриваются теорией игр. В ней различают игры людей между собой и игры людей с природой. Если в играх людей противоборствующие стороны являются активными и каждая из них выбирает стратегию, ухудшающую положение противоположной стороны, то природа представляет пассивную сторону, действия которой рассматриваются как случайные.

Среди стихийных сил, которые могут в случае возникновения оказать воздействие на носитель информации, наибольшую угрозу создает пожар. Он наиболее часто происходит, может полностью уничтожить носители информации, его тушение может сопровождаться залитием мест пожара водой и пеной с не менее разрушительными для носителя информации последствиями.

В соответствии со статьей 1 Закона РФ «О пожарной безопасности» пожар — неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства». Под горением понимается сложная физико-химическая реакция окисления, сопровождающаяся выделением тепла и дыма, появлением пламени или тления. Для возникновения горения необходимо наличие «треугольника горения»: горючей среды, источника зажигания и окислителя.

**Горючей средой** могут быть вещества в твердом, жидком и газообразном состоянии, в том числе:

- горючие элементы несущих, ограждающих и другие конструктивные элементы части здания (обрешетка чердаков, оконные переплеты, двери);
- горючие элементы оборудования (шланги, провода и др.);
- сырье, материалы, и горючая готовая продукция;
- горючая начинка здания (мебель, материалы и др.).

**Источники зажигания** — это горящие или накаленные тела, электрические разряды, обладающие запасом энергии и имеющие температуру, достаточные для возникновения горения. Типичными источниками зажигания являются:

- открытое пламя от костров, спичек, технологического оборудования, паяльных ламп, газовых горелок, горящей изоляции и др.;
- тление горючих веществ (табака, торфа, хлопка в упаковке и др.);

- нагретые поверхности технологического оборудования, дымовых труб, нагревательных элементов электроплит или электрочайников, токоведущих жил кабелей при перегрузке, отопительных приборов и оборудования и др.;
- экзотермические процессы, приводящие к тепловому, микробиологическому и химическому возгоранию;
- малоразмерные сильно нагретые тела в виде раскаленных частиц, возникающих при электрогазосварочных работах и коротком замыкании цепей электропитания, тлеющие табачные изделия, искры от костров, труб, автотранспорта и др.;
- электрические искры и дуги, возникающие в электрооборудовании при выключении, в неплотных контактах электрических соединений, статического электричества, молнии.

**Окислителем горения** служит кислород воздуха. Его снижение в замкнутом пространстве (помещении) замедляет процесс горения, а при понижении кислорода в воздухе ниже 15% горение прекращается. Это обстоятельство положено в основу тушения пожара путем уменьшения доступа кислорода к источнику горения. Однако для эффективного тушения пожара необходимо, чтобы огнетушащее вещество не вступало в реакции с горючей средой и не способствовало развитию пожара. В зависимости от горючей среды пожары разделяются на следующие классы:

- A — твердые горючие вещества (древесина, хлопок, торф, резинотехнические изделия, пластмассы);
- B — углеводороды, спирты, эфиры, альдегиды и кетоны (нефть, бензин, жиры, смолы, ацетон и др.);
- C — горючие газы (метан, пропан, водород, ацетилен и др.);
- D — легкие и щелочные металлы и их соединения (магний, калий, натрий, алюминий и др.);
- E — радио- и электрическое оборудование под электрическим напряжением.

Источниками угроз пожара, наводнения, механических разрушений могут быть не только природные явления, но и плоды недобросовестной деятельности человека, который своевременно не ремонтирует здания, помещения и их инфраструктуру. Наиболее частой причиной пожара в зданиях называют короткое замыкание между проводами электропроводки, которое возникает, прежде всего, из-за разрушения вследствие старения изоляции проводов.

Проржавевшие трубы водо- и теплоснабжения в случае их прорыва могут вызвать наводнение, особенно разрушительное в случае горячей воды.

Обратной стороной усложнения технических средств обработки, передачи и хранения информации, постоянно внедряемых во все сферы деятельности и жизни людей, является проблема их надежности. Скрытые дефекты в элементах, медленно текущие химические процессы в местах контакта и другие факторы все чаще проявляются с ростом сложности радиоэлектронных средств. Хотя принимаются достаточно серьезные меры по обеспечению их надежности, выявить все скрытые дефекты невозможно. Достаточно сослаться на опыт природы, которая для поддержания жизни живого существа постоянно обновляет его клетки и создала в его организме мощнейшую иммунную систему для борьбы с чужеродными вторжениями. Но даже эти меры, недостижимые для технических средств, далеко не всегда спасают живое существо от болезней с тяжелыми или трагическими последствиями.

Проблема усложняется еще тем обстоятельством, что вызванные неисправностями сбои в работе сложных радиоэлектронных средств не всегда оперативно выявляются, а могут проявиться в виде отложенных ошибок в работе. Например, сбои в работе процессора, вызванные чрезмерным повышением его температуры, можно заметить лишь по увеличению частоты его зависания. Учитывая, что сбой в аппаратуре — это изменение электрического сигнала, то изменение информационного сигнала приводит к изменению или даже к уничтожению информации, а изменение служебного сигнала — к блокированию информации.

Аналогичная картина наблюдается с программным обеспечением. Трудозатраты на нахождение ошибок большой программы сравнимы с трудозатратами на ее разработку. Поэтому производители программ подключают к их тестированию пользователей программ, собирая от них выявленные ими ошибки и внося исправления в очередную версию. Помимо ошибок в программе изменения и уничтожения информации вызывают вирусы, которые по мере роста их разновидностей создают серьезные угрозы безопасности информации.

Неквалифицированный или нерадивый работник представляет собой постоянную угрозу для обслуживаемой им аппаратуры и

циркулирующей в ней информации. Хотя у него нет плохих намерений, но своими действиями он может причинить урон, не меньший, чем от действий врага. Поговорка «добрыми намерениями вымощена дорога в ад» относится и к таким людям. Достаточно вспомнить, что страшнейшая в истории человечества чернобыльская катастрофа произошла из-за благих намерений повысить эффективность атомного реактора людьми, не рассмотревшими все возможные последствия проводимого ими эксперимента.

Грызуны, живущие в помещениях, где находятся средства обработки информации, могут привести их в такое состояние, при котором уничтожается или видоизменяется хранящаяся в них информация. Из истории перестройки известны факты, когда крысы, объедая изоляцию проводов, превращали в металлолом корабли и самолеты. Сбои в работе аппаратуры вызывают даже тараканы, которые с удовольствием устраивают свои колонии в темных и теплых пустотах радиоэлектронной аппаратуры, изменяя своими телами параметры ее элементов и цепей.

Так как утечка информации по акустическому, оптическому и радиоэлектронному техническим каналам происходит с помощью сигналов, в информационные параметры которых записывается защищаемая информация, то источниками угроз утечки являются, прежде всего, источники сигналов в этих каналах.

Утечка информации на носителях в виде материальных тел возникает при их несанкционированном и непреднамеренном переносе к злоумышленнику. Следует отличать утечку информации на материальных телах от несанкционированного, но преднамеренного переноса таких носителей, осуществляемого злоумышленником (агентом разведки или завербованным ею сотрудником). Например, лист документа, забракованный секретаршей при печатании и выброшенный ею в корзину для бумаг, может быть перенесен уборщицей в бак для отходов, вывезен на свалку за пределы организации. На свалке он может быть обнаружен злоумышленником, следящим за отходами организации. Этот процесс распространения носителя можно рассматривать как утечку информации. Если же этот документ целенаправленно выносится из организации с целью добывания из него информации, то информация добывается агентурными методами.

## 4.3. Опасные сигналы и их источники

Носители информации в виде полей и электрического тока называются **сигналами**. Если информация, содержащаяся в сигналах, секретная или конфиденциальная, а сигналы могут быть приняты (перехвачены, подслушаны) злоумышленником и с них, в принципе, может быть «снята» эта информация, то такие сигналы представляют опасность для информации и называются **опасными**.

Опасные сигналы могут быть **функциональными** и **случайными**.

**Функциональные сигналы** создаются для выполнения радиосредством заданных функций по обработке, передаче и хранении информации. При передаче закрытой информации функциональными сигналами ее отправитель осознает потенциальные угрозы безопасности содержащейся в сигналах информации. Принимает он необходимые меры или нет, это его выбор. По небрежности или злому умыслу, он иногда пренебрегает этими мерами. Например, на раннем этапе становления рыночных отношений бизнесмены часто по радиотелефонной сотовой связи разглашали сведения, составляющие коммерческую тайну. Более опытные люди при разговоре по открытой телефонной линии для скрытия от посторонних ушей некоторых аспектов разговора применяют так называемый «эзоповский» язык, т. е. слова со скрытым смыслом, не всегда понятным посторонним лицам.

К основным источникам функциональных сигналов относятся:

- передатчики (источники сигналов) систем связи;
- передатчики радиотехнических систем;
- излучатели акустических сигналов гидролокаторов и акустической связи;
- люди как источники условных сигналов.

**Средства систем связи** образуют наиболее многочисленную и разнообразную группу источников сигналов с семантической информацией. К системам и средствам связи относятся системы и средства радиосвязи, проводной, радиорелейной, космической и оптической связи, ионосферной, тропосферной и метеорной ра-

диосвязи. Они занимают ведущее место в обеспечении информационного обмена во всех сферах общественно-производственной деятельности и личной жизни людей.

Источниками радиосигналов, излучаемых в окружающее пространство, являются стационарные и мобильные радиопередающие устройства систем радиосвязи, а электрических сигналов, передаваемых по проводам, — телефонные, телеграфные, факсимильные аппараты, ПЭВМ, объединенные в сети, модемы аппаратуры передачи данных, телевизионные камеры кабельного телевидения и др.

В последнее время для передачи информации в качестве источников сигналов применяются также лазеры оптических средств связи. Уступая радиосигналам по дальности распространения, в особенности при неблагоприятных климатических условиях, оптические системы связи имеют значительно лучшие параметры по полосе пропускания и помехоустойчивости. Кабели волоконно-оптических линий связи с широкими возможностями по уменьшению величины затухания света и снижения себестоимости изготовления постепенно вытеснят металлические кабели проводных систем электросвязи.

Радио-, электрические и световые сигналы циркулируют как внутри организации, так и распространяются на большие, а при их ретрансляции — на любые расстояния. По телефону можно переговорить с абонентом в любом месте Земли, радиосигналы соответствующей частоты и мощности способны донести информацию также до любой ее точки.

Учитывая широкое применение средств связи и большие дальности распространения сигналов, перехват сигналов средств связи представляет один из эффективных и широко распространенных методов добывания информации. Сигналы средств связи содержат не только семантическую информацию, но и информацию о признаках сигналов и местоположении их источников. Такая информация характеризует технические решения новых средств и их возможности, что представляет интерес как для внутреннего, так и для внешнего (зарубежного) конкурента.

К **радиотехническим системам и средствам** относятся средства радиолокации, радионавигации, радиотелеметрии, радиотеле-

управления, а также радиопротиводействия (радиоэлектронной борьбы).

Среди радиотехнических систем и средств значительную долю занимают радиолокационные станции, предназначенные для наблюдения воздушного пространства и земной поверхности в радиодиапазоне. Возможности радиолокаторов по добыванию информации определяются в основном характеристиками радиотехнических сигналов и распределением их энергии в пространстве (диаграммой направленности). К радиотехническим системам и средствам, характеристики сигналов которых интересуют органы добывания разведки, относятся также **системы и средства радиопротиводействия (радиоэлектронной борьбы)**, предназначенные для нарушения систем управления войсками и оружием противника в военное время.

Так как радио- и гидролокационные станции создают техническую основу для противоракетной, противовоздушной и противолодочной обороны, то параметры сигналов новейших локаторов вызывают большой интерес у разведки других государств. Очевидно, что сигнальные признаки разрабатываемых радио- и акустических средств интересуют также конкурентов в России и других государствах, создающих подобную технику.

**Радионавигационные средства и системы** предназначены для определения местоположения объектов на суше, воде, в воздухе и в космосе. Радиотелеметрические средства и системы обеспечивают измерение и передачу различных физических величин удаленных объектов, а средства и системы радиотелеуправления — управление ими.

Передача коротких сообщений производится также **условными сигналами**. В качестве сигналов могут использоваться любые объекты наблюдения и излучения. Необходима только предварительная договоренность между источниками и получателями информации о содержании условного сигнала. Например, условными фразами часто пользуются люди во время конфиденциального разговора по открытому телефону, условными сигналами (паролями) обмениваются незнакомые люди при конфиденциальной встрече.

Но потенциальная опасность для информации, содержащейся в функциональных сигналах, априори известна ее владельцу. Он

при распространении сигналов или идет на осознанный риск, или может принять меры по его снижения до допустимого значения. Риск уничтожения, изменения или хищения информации — это та цена, которую объективно платит владелец информации для ее передачи современными способами. Он может передать информацию не с помощью сигналов, а с почтой или курьером, что часто делается, если цена информации очень высока, например при доставке дипломатических документов. Но при этом резко возрастают финансовые затраты и снижается оперативность. Поэтому электронные формы хранения и передачи информации вытесняют традиционные — на материальных телах.

Однако работа радиоэлектронных средств, используемых для приема, обработки, хранения и передачи сигналов, а также различных электрических приборов сопровождается явлениями и физическими процессами, которые могут создавать побочные радио- и электрические сигналы. Если эти сигналы по тем или иным причинам могут содержать секретную или конфиденциальную информацию и к ним возможен доступ технических средств злоумышленника, то опасность для этой информации существенно выше, чем для аналогичной информации, но содержащейся в функциональных сигналах. Такие случайно возникающие сигналы называются **случайными опасными сигналами**. Эти сигналы возникают в силу объективных физических процессов, часто независимо от пользователя технического средства. Без проведения специальных исследований его пользователь может и не знать о наличии случайных сигналов и тех угроз, которым подвергается секретная или конфиденциальная информация. В этом состоит существенное отличие функциональных опасных сигналов от случайных опасных сигналов.

К техническим средствам обработки, передачи и хранения, создающим опасные сигналы, относятся:

- средства телефонной проводной связи;
- средства мобильной телефонной и радиосвязи;
- средства электронной почты;
- средства электронной вычислительной техники;
- аудиоаппаратура и средства звукоусиления;
- радиоприемные устройства;

- видеоаппаратура;
- телевизионные средства;
- средства линейной радиотрансляции и оповещения.

Кроме того, случайные опасные сигналы создают электрические приборы, в том числе:

- средства системы электрочасофикации;
- средства охранной сигнализации;
- средства пожарной сигнализации;
- средства размножения документов;
- средства системы кондиционирования и вентиляции воздуха;
- бытовые приборы, оргтехника и иное производственное оборудование, имеющее в своем составе элементы преобразования акустической информации в электрические сигналы (акустоэлектрические преобразователи);
- электропроводящие коммуникации здания, проходящие через контролируемую зону.

Характеристики опасных случайных сигналов радиоэлектронных средств и электрических приборов априори неизвестны ни злоумышленнику, ни их пользователю. Для их обнаружения и определения характеристик проводят специальные проверки и исследования этих средств и приборов.

В зависимости от принадлежности циркулирующей (обрабатываемой, хранящейся, передаваемой) в технических средствах и системах информации к секретной (конфиденциальной) или несекретной эти средства и системы делятся на **основные технические средства и системы (ОТСС)** и **вспомогательные технические средства и системы (ВТСС)**.

К основным техническим средствам и системам относятся средства (системы) и их коммуникации (линии связи), обеспечивающие обработку, хранение и передачу защищаемой информации. Из этого не следует, что ОТСС должны обрабатывать только защищаемую информацию. В условиях рынка это экономически нецелесообразно. В общем случае ОТСС могут использоваться для решения задач, не связанных с сохранением тайны, но в них априори приняты меры по защите информации. Если в технических средствах (системах) приема, обработки, хранения и передачи инфор-

мации такие меры отсутствуют, то они относятся к вспомогательным. Вспомогательные технические средства и системы (ВТСС) не предназначены для обработки защищаемой информации, но могут размещаться совместно с ОТСС в контролируемой зоне. Последнее замечание имеет принципиальное значение, так как именно близость размещения ВТСС к ОТСС вынуждает рассматривать вспомогательные средства и системы как потенциальные источники опасных сигналов. Из сравнения назначения ОТСС и ВТСС следует, что множества ОТСС и ВТСС пересекаются. Действительно, в одном помещении могут размещаться средства, например, однотипные компьютеры, часть из которых являются основными, другие — вспомогательные. Вспомогательный компьютер может быть подключен к интегральной сети общего пользования, например к Internet, что нельзя делать для компьютера, относящегося к основному средству обработки информации. В [29] к ВТСС отнесены:

- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
  средства и системы кондиционирования;
  средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания и радиоприемники и т. д.);
- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

### Вопросы для самопроверки

1. Сущность угрозы безопасности информации.
2. Виды угроз безопасности информации и их отличия.
3. Основные угрозы воздействия на источники информации и ее утечки.
4. Основные источники угроз информации, содержащей государственную тайну.

5. Факторы, влияющие на риск угрозы безопасности информации.
6. Чем отличаются опасные случайные сигналы от функциональных опасных сигналов?
7. Основные источники опасных случайных сигналов.
8. Классы пожаров.
9. Чем отличаются основные технические средства и системы от вспомогательных технических средств и систем?

# Глава 5. Побочные электромагнитные излучения и наводки

Физическую основу случайных опасных сигналов, возникающих во время работы в выделенном помещении радиосредств и электрических приборов, составляют **побочные электромагнитные излучения и наводки (ПЭМИН)**. Процессы и явления, образующие ПЭМИН, по способам возникновения можно разделить на 4 вида:

- не предусмотренные функциями радиосредств и электрических приборов преобразования внешних акустических сигналов в электрические сигналы;
- паразитные связи и наводки;
- побочные низкочастотные излучения;
- побочные высокочастотные излучения.

За рубежом побочные электромагнитные излучения называют «компрометирующими» излучениями (compromising emanations). Факты побочных излучений отмечены еще в XIX веке. Например, в 1884 г. в телефонных аппаратах на улице Грей-Стоун-Род в Лондоне прослушивались телеграфные сигналы, излучаемые неглубоко и параллельно проложенными под землей телеграфными проводами. Первые работы по изучению этих излучений появились еще в 20-е годы, но полномасштабные исследования их начались с 40–50-х годов XX века. Этому способствовало то, что развитие радиоприемной техники к этому времени создало возможности по практическому добыванию информации из побочных излучений. Например, после Второй мировой войны американскими спецслужбами были обнаружены побочные излучения и восстановлен в результате их перехвата информационный сигнал телетайпа советского представительства в Берлине. С середины 80-х годов постоянно растет количество по этой проблеме не только закрытых, но и открытых публикаций.

## 5.1. Побочные преобразования акустических сигналов в электрические сигналы

Преобразователи внешних акустических сигналов в электрические сигналы называются **акустоэлектрическими преобразователями**. К акустоэлектрическим преобразователям относятся физические устройства, элементы, детали и материалы, способные под действием переменного давления акустической волны создавать эквивалентные электрические сигналы или изменять свои параметры. Классификация акустоэлектрических преобразователей по физическим процессам, создающим опасные сигналы, приведена на рис. 5.1.

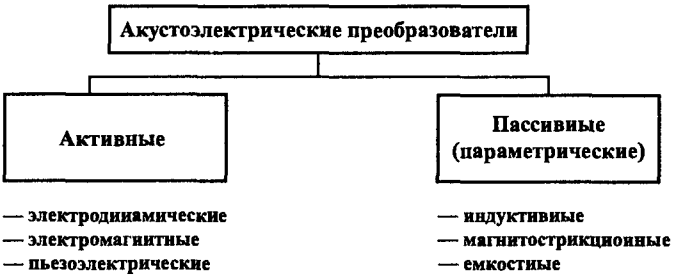



*Рис. 5.1.* Классификация акустоэлектрических преобразователей

На выходе активных акустоэлектрических преобразователей под действием акустической волны возникают электрические сигналы. У пассивных акустоэлсктрических преобразователей те же действия акустической волны вызывают лишь изменения параметров преобразователей.

По способам формирования электрического сигнала активные акустоэлектрические преобразователи могут быть **электродинамическими, электромагнитными и пьезоэлектрическими**.

Опасные сигналы в **электродинамических акустоэлектрических преобразователях** возникают в соответствии с законом электромагнитной индукции при перемещении провода в магнитном поле под действием акустической волны (рис. 5.2).

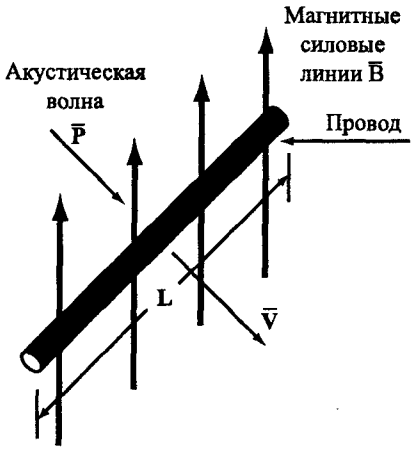



*Рис. 5.2.* Принципы работы электродинамического акустоэлектрического преобразователя

Если провод длиной L под действием акустической волны со звуковым давлением P перемещается со скоростью V в магнитном поле с индукцией B, то в нем при условии перпендикулярности силовых магнитных линий проводу и скорости его перемещения, возникает ЭДС величиной $\varepsilon = LBV$. Так как $V = PS/Z_{мс}$ (P — звуковое давление, S — площадь провода, на которую оказывает давление акустическая волна, $Z_{мс}$ — величина механического сопротивления движению провода), то $\varepsilon = LBSP / Z_{мс}$.

Наибольшей чувствительностью обладают электродинамические акустоэлектрические преобразователи в виде динамических головок громкоговорителей (см. рис. 5.3).

Сущность преобразования состоит в следующем. Под давлением акустической волны соединенная с диффузором катушка в виде картонного цилиндра с намотанной на нем тонкой проволокой перемещается в магнитном поле, создаваемом постоянным магнитом цилиндрической формы. В соответствии с законом электромагнитной индукции в проводах катушки возникает электродвижущая сила (ЭДС), величина которой пропорциональна громкости звука.

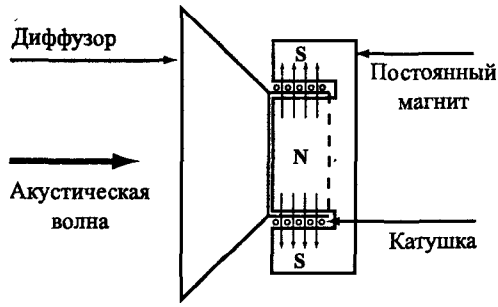



*Рис. 5.3.* Схема электродинамического громкоговорителя

Аналогичный эффект возникает в **электромагнитных акустоэлектрических преобразователях**. К ним относятся электромагниты электромеханических звонков и капсюлей телефонных аппаратов, шаговые двигатели вторичных часов, кнопочные извещатели ручного вызова пожарной службы охраняемого объекта и др. Электрические сигналы индуцируются в катушках электромагнитов этих устройств в результате изменений напряженности создаваемых ими полей, вызванных изменениями под действием акустической волны воздушного зазора между сердечником и якорем электромагнита или статора (неподвижной части) и ротора (подвижной) части электродвигателя. Для приведенной на рис. 5.4 схемы электромагнитного акустоэлектрического преобразователя напряжение E на концах проволоки, намотанной на катушке, пропорционально количеству витков W, площади s и относительной магнитной проницательности $\mu_0$ сердечника, обратно пропорционально расстоянию $\Delta$ между полюсом сердечника и подвижного якоря.

Перечень бытовых радио- и электроприборов, в которых возникают подобные процессы и которые устанавливаются в служебных и жилых помещениях, достаточно велик. К ним относятся: телефонные аппараты с электромеханическими звонками, вторичные электрические часы системы единого времени предприятия или организации, вентиляторы и др. Уровни опасных сигналов в этих цепях зависят от конструкции конкретного типа средства и их значения имеют значительный разброс. Например, опасные сигналы, создаваемые звонковой цепью телефонного аппарата, могут достигать значений долей и единиц мВ.

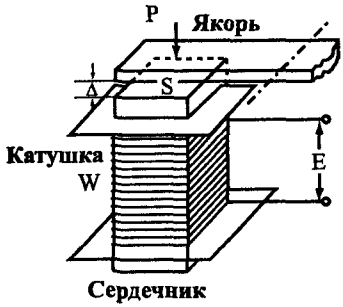



*Рис. 5.4.* Схема электромагнитного акустоэлектрического преобразователя

**Активными акустоэлектрическими преобразователями** являются также некоторые кристаллические вещества (кварц, сегнетовая соль, титанат и ниобат бария и др.), которые широко применяются в радиоаппаратуре для стабилизации частоты и фильтрации сигналов, в качестве акустических излучателей сигналов вызова в современных телефонных аппаратах вместо электромеханических звонков. На поверхности этих веществ при механической деформации их кристаллической решетки (давлении на поверхность, изгибе, кручении) возникают электрические заряды.

В **пассивных акустоэлектрических преобразователях** акустическая волна изменяет параметры элементов схем средств, в результате чего изменяются параметры циркулирующих в этих схемах электрических сигналов. В большинстве случаях под действием акустической волны изменяются параметры индуктивностей и емкостей электрических цепей. В соответствии с этим акустоэлектрические преобразователи называются **индуктивными** и **емкостными**.

Если схема электрической цепи содержит катушку с витками проволоки, то под действием акустической волны изменяются расстояние между витками и геометрические размеры самой катушки. В результате этого, как следует из соответствующих формул, изменяется индуктивность катушки. Если, например, катушка является элементом частотно-задающего контура генератора, то изменение индуктивности вызывает частотную модуляцию сигнала генератора. В итоге информация, записанная в параметры акустической

волны, переписывается в параметры электрического сигнала, способного перенести ее к злоумышленнику на большое расстояние. Аналогичная картина наблюдается при изменении под действием акустической волны емкости контура генератора.

Если акустоэлектрический преобразователь представляет собой реактивное сопротивление, величина которого меняется в соответствии с параметрами акустического сигнала, то изменение этого сопротивления вызывает амплитудную модуляцию тока в цепи.

Разновидностью индуктивного является магнитострикционный акустоэлектрический преобразователь. **Магнитострикция** проявляется в изменении магнитных свойств ферромагнитных веществ (электротехнической стали и ее сплавов) при их деформировании (растяжении, сжатии, изгибании, кручении). Такое явление называется Виллари-эффектом или обратной магнитострикцией, открытым итальянским физиком Э. Виллари в 1865 г. Этот эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика. Прямая магнитострикция заключается в изменении геометрических размеров и объема ферромагнитного тела при помещении его в магнитное поле. В результате обратной магнитострикции под действием акустической волны изменяется магнитная проницаемость сердечников контуров, дросселей, трансформаторов радио- и электротехнических устройств, что приводит к эквивалентному изменению значений индуктивностей цепи и модуляции протекающих через них высокочастотных сигналов.

К наиболее распространенным случайным акустоэлектрическим преобразователям относятся:

- вызывные устройства телефонных аппаратов;
- динамические головки громкоговорителей, электромагнитные капсюли телефонных трубок, электрические двигатели вторичных часов системы единого времени и бытовых электроприборов;
- катушки контуров, дросселей, трансформаторов, провода монтажных жгутов, пластины (электроды) конденсаторов;
- пьезоэлектрические вещества (кварцы генераторов, виброакустические излучатели акустических генераторов помех);

- ферромагнитные материалы в виде сердечников трансформаторов и дросселей.

Угроза информации от акустоэлектрического преобразователя зависит, прежде всего, от его чувствительности. **Чувствительность** акустоэлектрического преобразователя характеризуется отношением величины электрического сигнала на его выходе или изменения падающего на нем напряжения к силе звукового давления на поверхность чувствительного элемента преобразователя на частоте f = 1000 кГц и измеряется в В/Па или мВ/Па. Очевидно, что чем выше чувствительность случайного акустоэлектрического преобразователя, тем больше потенциальная угроза от него для безопасности акустической информации.

Чувствительность в мВ/Па некоторых акустоэлектрических преобразователей приведена в табл. 5.1 [11].

Опасные сигналы, образованные акустоэлектрическими преобразователями, могут:

- распространяться по проводам, выходящим за пределы контролируемой зоны;
- излучаться в эфир;
- модулировать другие, более мощные электрические сигналы, к которым возможен доступ злоумышленников.

*Таблица 5.1*

| *№ п/п* | *Акустоэлектрический преобразователь* | *Чувствительность, мВ/Па* |
|---|---|---|
| 1 | Электродинамический микрофон | 4–6 |
| 2 | Электродинамический громкоговоритель | 2–3 |
| 3 | Абонентский громкоговоритель | 30–45 |
| 4 | Вторичные электрические часы | 0,1–0,5 |
| 5 | Электромеханический звонок телефонного аппарата | 0,05–0,6 |
| 6 | Пьезоэлектрическое вызывное устройство телефонного аппарата | 8–11 |
| 7 | Телефонный капсюль | 3–5 |
| 8 | Электромагнитное реле | 0,04–0,5 |
| 9 | Трансформаторы, дроссели | 0,001–0,2 |

Техническую основу для реализации первой угрозы создают, например, неработающий громкоговоритель городской ретрансляционной сети и звонковая цепь телефонных аппаратов устаревших, но широко еще применяемых типов (ТА-68М, ТА-72М, ТАН-70-2, ТАН-76-3, ТА-1146, ТА-1162, ТА-1164 и др.). Головка громкоговорителя непосредственно подключается к кабелю (двухжильному проводу) при приеме первой программы городской ретрансляционной сети через согласующий трансформатор, который повышает амплитуду опасных сигналов до 30–40 мВ. Сигнал такой амплитуды может распространяться по проводам ретрансляционной сети на значительные расстояния, достаточные для снятия информации злоумышленником за пределами территории организации. Однако если в радиотрансляционной сети идет передача речи или музыки, то сигналы этой передачи, имеющие существенно большую (в 100–200 раз) амплитуду и совпадающий диапазон частот, подавляют опасные сигналы. Поэтому работающие громкоговорители, может быть, и мешают работе людей, но исключают утечку информации из помещений через акустоэлектрические преобразователи в громкоговорителях.

Иная ситуация с акустоэлектрическими преобразователями в телефонных аппаратах. Телефонные линии постоянно подключены к источнику тока напряжением порядка 60 В. Хотя опасные сигналы на выходе звонковой сети составляют единицы и доли мВ, их нетрудно отделить с помощью фильтра от значительно более высокого напряжения постоянного тока в телефонной линии. Постоянный ток фильтр не пропускает, а опасные сигналы с речевой информацией от акустоэлектрических преобразователей с частотами в звуковом диапазоне проходят через фильтр с малым ослаблением, а затем усиливаются до необходимого значения.

Опасными сигналами на выходе акустоэлектрических преобразователей, имеющими даже весьма малые значения (доли милливольт), нельзя пренебрегать. Во-первых, чувствительность современных радиоприемников и усилителей электрических сигналов превышает в десятки и сотни раз уровни наиболее распространенных опасных сигналов, а, во-вторых, маломощные опасные сигналы могут модулировать более мощные электрические сигналы и поля и таким образом увеличивать дальность распространения

опасных сигналов. Например, если опасные сигналы попадают в цепи генераторов (гетеродинов) любого радио- или телевизионного приемника, то они модулируют гармонические колебания этих генераторов по амплитуде или частоте и распространяются за пределы помещения уже в виде электромагнитной волны. Также поля опасных сигналов на выходе акустоэлектрических преобразователей, которые сами по себе из-за малой напряженности не несут большой угрозы безопасности информации, могут наводить в цепях рядом расположенных радиоэлектронных средств электрические сигналы с аналогичным эффектом.

## 5.2. Паразитные связи и наводки

В любом радиоэлектронном средстве или электрическом приборе наряду с токопроводами (проводами, проводниками печатных плат), предусмотренными их схемами, возникают многочисленные побочные пути, по которым распространяются электрические сигналы, в том числе опасные сигналы акустоэлектрических преобразователей. Эти пути создаются в результате паразитных связей и наводок. Первопричиной их являются поля, создаваемые электрическими зарядами и токами в цепях радиоэлектронных средств и приборов.

Постоянные электрические заряды и электрический ток в элементах и цепях радиосредств и электрических приборов создают соответствующие электрические и магнитные поля, а заряды и ток переменной частоты — электромагнитные поля. Поля распространяются в пространстве и воздействуют на элементы и цепи других технических средств и систем. Кроме того, для функционирования средств и систем необходимо обеспечить гальваническое соединение их элементов. Из-за гальванических соединений возникают дополнительные пути для распространения сигналов одних узлов и блоков по цепям других. В результате воздействия побочных полей и влияния через проводники и резисторы сигналов одних узлов и блоков на сигналы других блоков и узлов возникают паразитные связи и наводки как внутри радиоэлектронных средств, так и между рядом расположенными средствами. Эти связи и наводки ухудшают работу узлов, блоков и средств в целом. Поэтому при проектировании радиоэлектронных средств уровни этих пара-

зитных связей и наводок снижают до допустимых значений. Чем выше требования к характеристикам средств, тем требуются большие усилия, а следовательно, и затраты для нейтрализации паразитных связей и наводок. Основная часть высокой цены (десятки тысяч долларов) высокоточных контрольно-измерительных приборов фирм Hewlett Packard, Ronde & Scwarz и др. приходится на меры по уменьшению паразитных связей и наводок.

Однако несмотря на принимаемые меры по снижению уровня паразитных связей и наводок для обеспечения требуемых характеристик радиоэлектронного средства, остаточный их уровень создает угрозы для информации, содержащейся в информационных параметрах сигналов, циркулирующих в радиоэлектронном средстве. **Поэтому любое радиоэлектронное средство или электрический прибор следует с точки зрения информационной безопасности рассматривать как потенциальный источник угрозы безопасности информации.**

Известны три вида паразитных связей:

- емкостная;
- индуктивная;
- гальваническая.

**Емкостная связь** образуется в результате воздействия электрического поля, индуктивная — воздействия магнитного поля, гальваническая связь — через общее активное сопротивление.

Модель емкостной паразитной связи представлена на рис. 5.5.

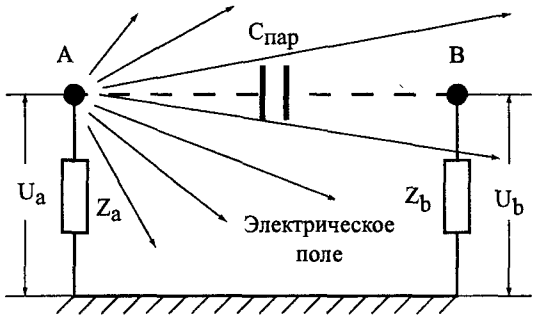



*Рис. 5.5.* Паразитная емкостная связь

На этом рисунке $U_a$ — потенциал заряда точки А относительно корпуса, создающий электрическое поле. В результате воздействия этого поля в точке В возникает заряд противоположного знака. Величина потенциала заряда (наведенного напряжения) $U_b$ точки В относительно корпуса определяется соотношением емкостного сопротивления $C_п$, и сопротивлений $Z_b$:

$$U_b = U_a \frac{Z_b}{Z_b + Z_п},$$

где $Z_п = 1 / j\omega C_п$ — емкостное сопротивление между точками А и В, $\omega$ — круговая частота изменения потенциала заряда точки А.

Емкость $C_п$ является паразитной и создает емкостную паразитную связь между точками А и В. Отношение $\beta_c = U_b / U_a = \frac{Z_b}{Z_b + Z_п}$ называется **коэффициентом паразитной емкостной связи**. В большинстве реальных случаев $Z_п >> Z_b$, поэтому $\beta_c \approx Z_в j\omega C_п$. Следовательно, коэффициент паразитной емкостной связи пропорционален величине паразитной емкости и частоте колебаний электрического поля.

Емкостная паразитная связь возникает между любыми элементами схемы: проводами, радиоэлементами схемы и корпусом (шасси). Величина паразитной емкости на единицу длины проводов, параллельно расположенных на удалении b друг от друга, определяется по формуле:

$$C_п \approx \frac{\pi \varepsilon_a}{\ln\left[\frac{2b}{d} + \sqrt{\left(\frac{b}{d}\right)^2 - 1}\right]},$$

где d — диаметр проводов; $\varepsilon_a$ — абсолютное значение диэлектрической постоянной.

Из этой формулы следует, что величина емкости пропорциональна диэлектрической проницаемости среды, диаметру проводов и обратно пропорциональна расстоянию между проводами. Максимальная паразитная емкость возникает между проводами

катушек, в которых витки проводов наматываются вплотную друг к другу ($b \approx d$) и пропитываются лаком ($\varepsilon_a \approx 4{,}5 \cdot 10^{-11}$ Ф/м). Эта емкость составляет $4{,}4 \cdot 10^{-10}$ Ф/м или 44 пФ/м. Емкость между двумя параллельными проводами длиной 100 мм и диаметром 0,1 мм уменьшается с 0,75 пф до 0,04 пф при увеличении расстояния между ними с 2 до 50 мм. Для проводов диаметром 2 мм эта емкость при тех же условиях больше и составляет 5–0,07 пф [12].

Так как между рядом расположенными основными и вспомогательными средствами существует паразитная емкостная связь, способствующая передаче сигналов с защищаемой информацией от ОТСС к ВТСС, то для определения величины наводки надо знать их паразитные емкости. Эти емкости называются **собственными емкостями** радиоэлектронного средства и электрического прибора. Вычислить собственную емкость можно только для простейших конфигураций типа штырь, шар, диск. Например, для штыря длиной L паразитная емкость составляет $C_п \approx 0{,}1L$, для диска $C_п \approx 0{,}35D$, шара — $C_п \approx 0{,}56D$, где D — диаметр шара и диска. Для реальных радиоэлектронных средств сложной конфигурации собственная емкость $C_п$ определяется экспериментально путем размещения средства в однородном электрическом поле и измерением наведенного напряжения на его выходе $U_н$. Предварительно измеряется наведенное эталонное напряжение $U_{пэ}$ в простейшем устройстве (диске, шаре и др.) с известной (эталонной) собственной емкостью $C_{пэ}$, помещенном в это поле. На основе полученных данных собственная емкость исследуемого средства определяется методом замещения, в соответствии с которым $C_п = C_{пэ}U_н/U_{пэ}$.

**Паразитная индуктивная связь** иллюстрируется рис. 5.6.

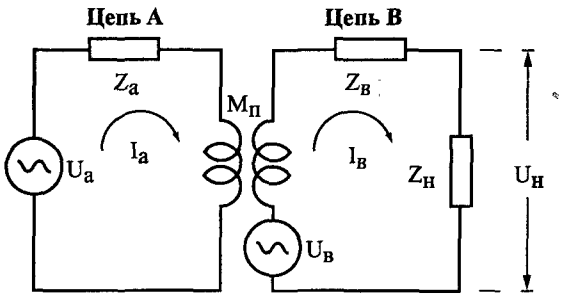



*Рис. 5.6.* Паразитная индуктивная связь

Переменный ток, протекающий по цепи А, создает магнитное поле, силовые линии которого достигают проводников другой цепи В и наводят в ней ЭДС величиной

$$U_в = I_а \omega M_п = U_а \omega M_п / Z_а,$$

где ω — круговая частота переменного тока в цепи А; $Z_а$ — полное сопротивление цепи А; $M_п$ — паразитная взаимная индуктивность между цепями А и В.

ЭДС величиной $U_в$ создает в цепи В ток $I_в$, обратно пропорциональный суммарному сопротивлению $Z_b$ цепи В и сопротивлению нагрузки $Z_н$. Этот ток вызывает на нагрузке напряжение наводки $U_н = U_в Z_н / (Z_в + Z_н) = U_а \omega M_п Z_н / Z_а (Z_в + Z_н)$. Отношение $\beta_и = U_н / U_а = \omega M_п Z_н / Z_а (Z_в + Z_н)$ называется **коэффициентом паразитной индуктивной связи**. Он, как следует из приведенного выражения, пропорционален частоте переменного тока и величине паразитной взаимной индуктивности и обратно пропорционален сопротивлению цепей.

Взаимная индуктивность замкнутых цепей зависит от взаимного расположения и конфигурации проводников. Она тем больше, чем большая часть магнитного поля тока в одной цепи пронизывает проводники другой цепи.

Следует различать взаимную индуктивность между проводниками разных цепей от индуктивности проводника. Индуктивность характеризует свойство проводника препятствовать изменению проходящего через него тока, которое обусловлено явлением *самоиндукции*. Она возникает, когда силовые линии переменного магнитного поля пронизывают проводники, по которым протекает ток, создающий это магнитное поле. Следовательно, переменное магнитное поле, как гоголевская унтер-офицерская вдова, способно само себя высечь.

**Гальваническую паразитную связь** еще называют связью через общее сопротивление, входящее в состав нескольких цепей. Такими общими сопротивлениями могут быть сопротивление соединительных проводов и устройств питания и управления. Например, узлы и блоки компьютера, осуществляющего обработку информации, соединены с напряжением +5 В блока питания. Для установки «0» триггеров дискретных устройств на соответс-

твующие их входы подается одновременно соответствующий сигнал управления. На рис. 5.7 приведена упрощенная схема, иллюстрирующая возникновение гальванической связи.

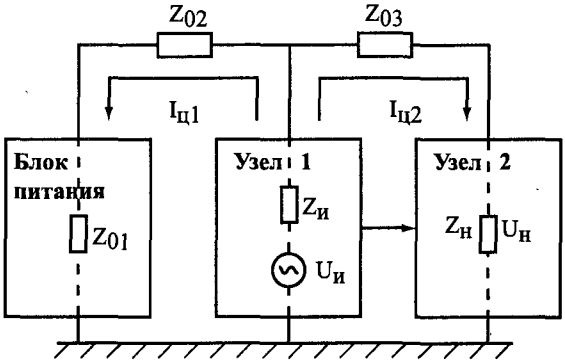



*Рис. 5.7.* Паразитная гальваническая связь

В соответствии с ним к блоку питания через общие сопротивления $Z_{01}$, $Z_{02}$ и $Z_{03}$ подключены узел 1 и узел 2 радиоэлектронного средства. Сигнал напряжением $U_и$ 1-го узла создает токи $I_{ц1}$ и $I_{ц2}$, в результате которых на эквивалентном сопротивлении $Z_н$ 2-го узла возникает напряжение наводки $U_н$. Отношение $\beta_г = U_н/U_и$ называется **коэффициентом паразитной гальванической связи**.

Если побочные поля и электрические токи являются носителями защищаемой информации, то паразитные наводки и связи могут приводить к утечке информации. Следовательно, паразитные связи и наводки представляют собой побочные физические процессы и явления, которые могут приводить к утечке защищаемой информации.

Возможность утечки информации через паразитные связи и наводки носит вероятностный характер и зависит от многих факторов, в том числе от конфигурации, размеров (относительно периода колебаний протекающих токов) и взаимного положения излучающих и принимающих токопроводящих элементов средств. В отличие от предусмотренных для связи функциональных антенн, конструкция и характеристики которых определяются при созда-

нии радиопередающих и радиоприемных средств, эти элементы можно назвать **случайными антеннами**.

Случайными антеннами могут быть монтажные провода, соединительные кабели, токопроводы печатных плат, выводы радиодеталей, металлические корпуса средств и приборов и другие элементы средств. Параметры случайных антенн существенно хуже функциональных. Но из-за небольших расстояний между передающими и приемными случайными антеннами (в радиоэлектронном средстве или одном помещении) они создают угрозы утечки информации.

Случайные антенны имеют сложную и часто априори неопределенную конфигурацию, достаточно точно рассчитать значения их электрических параметров, совпадающих с измеряемыми, очень сложно. Поэтому реальную случайную антенну заменяют ее моделями в виде проволочной антенны — отрезка провода (вибратора) и рамки.

В ближней зоне вибратор создает преимущественно электрическое поле. Свойства проволочной антенны преобразовать электрический сигнал в поле (радиосигнал) и наоборот характеризуются параметром антенны, названным **действующей высотой** $h_д$ и измеряемым в м. Действующая высота передающей антенны представляет собой параметр, связывающий напряженность электрического поля, создаваемого антенной в направлении главного излучения, с уровнем сигнала в самой антенне. Действующая высота приемной антенны равна отношению ЭДС в приемной антенне к напряженности вызывающего ее электрического поля: $h_д = U_а/E_а$. При этом предполагается, что приемная антенна ориентирована в пространстве в соответствии с поляризацией электромагнитного поля и прием осуществляется с направления максимального уровня поля. Так как отношение напряженностей электрической и магнитной составляющих электромагнитного поля возле случайной антенны равно волновому сопротивлению среды ($Z_в = E_а/H_а$), то $h_д = U_а/H_а Z_в$.

Коэффициент усиления случайной антенны в виде замкнутой цепи (рамки) оценивается с помощью параметра, названного

**действующей длиной антенны** $L_д = U_а/H_а$. По аналогии со способами определения собственной емкости средства действующая высота (длина) случайной антенны находится методом замещения.

Паразитные связи могут вызывать утечку информации по проводам и создавать условия для возникновения побочных электромагнитных излучений. За счет паразитных связей возникают опасные сигналы в проводах кабелей различных линий и цепей, в том числе в цепях заземления и электропитания, а также возникают паразитные колебания в усилителях, дискретных устройствах и др.

Серьезную угрозу безопасности информации создают наводки сигналов ОТСС на провода и кабели, выходящие за пределы контролируемой зоны (рис. 5.8). Когда ток проходит по проводникам первой цепи (Ц1), вокруг них создается магнитное поле, силовые линии которого пронизывают проводники второй цепи (Ц2). В результате этого по цепи Ц2 потечет помимо основного еще и переходной ток, создающий помеху основному. Защищенность от взаимных помех оценивается так называемым **переходным затуханием** $Z_{12} = 10\lg P_{с1}/P_{н2}$, где $P_{с1}$ и $P_{н2}$ — мощность сигналов в 1-й цепи и наводки от них во 2-й цепи. Для надежной защиты информации переходное затухание должно быть не менее величины $10\lg P_с/P_{пр}$, где $P_с$ и $P_{пр}$ — мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал. Так как кабели в здании укладываются в специальных колодцах и нишах, то между кабелями за счет их достаточно близкого и параллельного на большом расстоянии расположения возникают достаточно большие паразитные связи между кабелями внутренней и городской АТС, других информационных линий связи, цепями электропитания и заземления. Так как сотрудники организации при разговоре по телефонам внутренней АТС чаще допускают нарушения режима секретности (конфиденциальности), чем во время разговора по городской АТС, то при регулярном подслушивании разговоров по внутренней АТС можно добыть ценную информацию.

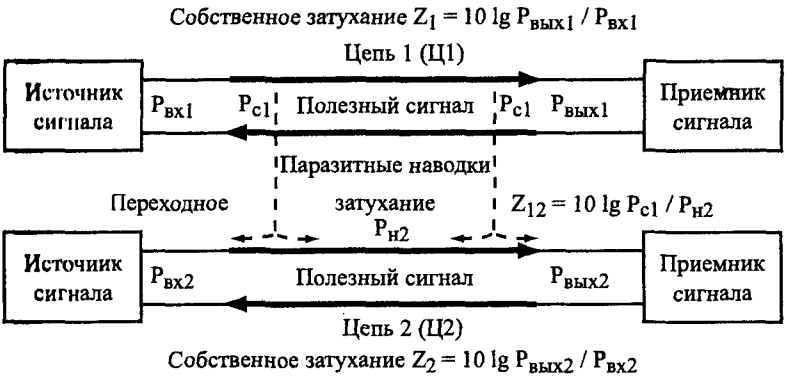



*Рис. 5.8.* Паразитные наводки

Современная архитектура служебных помещений предусматривает создание между межэтажными перекрытиями и потолком (полом) свободного пространства для прокладки различных кабелей (электропитания, внутренней и городской АТС, трансляции, оперативной и диспетчерской связи, сетей передачи данных и др.). Это создает дополнительные возможности для возникновения между проводами кабелей паразитных связей и появления опасных сигналов, распространяющихся за пределы контролируемой зоны.

## 5.3. Низкочастотные и высокочастотные излучения технических средств

Большую угрозу безопасности информации создают также побочные излучения радио- и электротехническими средствами электромагнитных полей, содержащих защищаемую информацию. Источниками излучений могут быть цепи, содержащие статические или динамические заряды (электрический ток), в информационные параметры которых тем или иным способом записывается защищаемая информация. Носители защищаемой информации в виде статических или динамических зарядов могут попадать в эти цепи непосредственно, если эти цепи участвуют в обработке, передаче и хранении защищаемой информации или сами элементы цепей обладают свойствами акустоэлектрических преобразователей,

или опосредованно, когда опасные сигналы проникают в излучающие цепи через паразитные связи.

Вид излучения и характер распространения электромагнитного поля в пространстве зависит от частоты колебаний поля и вида излучателя. Различают **низкочастотное и высокочастотные опасные излучения**.

Под низкочастотными излучениями понимаются излучения электромагнитных полей, частоты которых соответствуют звуковому диапазону. Источниками таких излучений являются устройства и цепи звукоусилительной аппаратуры (микрофоны, усилители мощности, аудиомагнитофоны, громкоговорители и их согласующие трансформаторы, кабели между микрофонами и усилителями, усилителями и громкоговорителями, цепи, содержащие случайные акустоэлектрические преобразователи, телефонные аппараты и кабели внутренней АТС и др.).

Наибольшую угрозу создают средства звукофикации помещений для озвучивания акустической информации, содержащей государственную или коммерческую тайну. Эти средства включают микрофоны, усилители мощности, громкоговорители, устанавливаемые на стенах больших помещений (залов для совещаний, конференц-залов) или в спинки кресел, а также соединительные кабели. Причем часто усилители мощности размещаются в техническом помещении, удаленном на значительном расстоянии от конференц-зала. По проводам кабелей звукоусилительной аппаратуры протекают большие токи, составляющие доли и единицы ампер. Эти токи создают мощные магнитные поля, которые, во-первых, могут распространяться за пределы выделенного помещения, здания и даже организации, а во-вторых, наводить ЭДС в любых токопроводящих конструкциях, в том числе в цепях электропитания и металлической арматуре зданий.

К **высокочастотным опасным излучениям** относятся электромагнитные поля, излучаемые цепями радиоэлектронных средств, по которым распространяются высокочастотные (выше звукового диапазона) сигналы с секретной (конфиденциальной) информацией. Можно утверждать, что если не приняты специальные дополнительные меры, то источниками подобных опасных побочных

ВЧ-излучений могут быть любые цепи радио- и электрических средств. К основным источникам побочных излучений с мощностью, достаточной для распространения электромагнитного поля за пределы контролируемой зоны, например помещения, относятся:

- гетеродины радио- и телевизионных приемников;
- генераторы подмагничивания и стирания аудио- и видеомагнитофонов;
- усилители и логические элементы в режиме паразитной генерации;
- электронно-лучевые трубки средств отображения защищаемой информации (мониторов, телевизоров);
- элементы ВЧ-навязывания;
- мониторы, клавиатура, принтеры и другие устройства компьютеров, в которых циркулируют сигналы в параллельном коде.

**Гетеродины радио- и телевизионных приемников** являются генераторами гармонических колебаний, необходимыми для преобразования частоты принимаемого сигнала в промежуточную частоту. Гармоническое колебание с гетеродина подается на смеситель, на нелинейном элементе (диоде или транзисторе) которого осуществляется преобразование входного (принимаемого) сигнала в сигнал промежуточной частоты. Частоты сигналов гетеродинов отличаются на величину промежуточной частоты (465 кГц — для ДВ-, СВ- и КВ-диапазонов, 10 МГц — для УКВ-диапазонов) от принимаемых сигналов и могут иметь значения от сотен кГц до десятков ГГц. Если элементы контура (индуктивность и емкость) гетеродина обладают свойствами акустоэлектрических преобразователей или в него проникают опасные сигналы от других акустоэлектрических преобразователей, то возможна амплитудная или частотная модуляция сигналов гетеродина. Мощность излучения модулированных сигналов гетеродина тем больше, чем ближе значения длины волны гармонического колебания к длине цепей, по которым протекают сигналы гетеродинов. Часто она бывает достаточной для подслушивания речевой информации в кабинете руководителя с включенным радио- или телевизионным приемником с помощью бытовых радиоприемников в соседних помещениях или даже зданиях.

**Генераторы сигналов высокочастотного подмагничивания и стирания** магнитофонов создают гармонические колебания на частотах в сотни кГц. Генераторы сигналов высокочастотного подмагничивания необходимы для обеспечения аналоговой аудио- и видеозаписи с малыми нелинейными искажениями. Зависимость остаточной намагниченности магнитной пленки от напряженности магнитного поля в головке записи нелинейная, что вызывает нелинейные искажения в записанном сигнале. Путем подачи в магнитную головку наряду с током записи дополнительного тока подмагничивания с частотой около 100 кГц и амплитудой, в 6–8 раз превышающей максимальную амплитуду тока записи, устанавливается рабочая точка для тока записи на линейном участке кривой намагничивания магнитной ленты. В результате выбора оптимального тока подмагничивания удается уменьшить нелинейные искажения сигналов записи до единиц процентов.

Генератор высокочастотного стирания обеспечивает стирание записанной на магнитную ленту информации путем размагничивания ее магнитного слоя практически до нуля. Для этого в стирающую головку аудиомагнитофона подается ток с частотой 50–100 кГц. При такой частоте тока стирания и уменьшения напряженности магнитного поля головки в результате удаления стираемого элементарного участка движущейся магнитной ленты от зазора стирающей магнитной головки происходит многократное перемагничивание участка с убывающей до нуля намагниченностью. В отличие от высокочастотного стирания уничтожение информации путем воздействия на магнитный слой магнитным полем постоянного магнита, который применяется в качестве стирающей головки в специальных диктофонах, обеспечивается путем намагниченности магнитного слоя ленты до насыщения.

**Паразитная генерация** может возникнуть при определенных условиях в усилителях и логических элементах дискретной техники. Логический элемент рассматривается в данном контексте как усилитель с очень высоким коэффициентом усиления.

Математическую модель усилителя независимо от числа каскадов усиления можно представить в виде комплексной передаточной функции $K_{ус}(\omega)e^{j\varphi_{ус}(\omega)}$, где $K_{ус}(\omega)$ и $\varphi_{ус}(\omega)$ — зависящие от частоты $\omega = 2\pi f$ коэффициент усиления и фаза выходного сигнала по

отношению к входному. В усилителе напряжения фаза выходного сигнала для нечетного числа каскадов усиления изменяется на 180°, а при четном числе каскадов совпадает с фазой входного сигнала.

Так как между элементами усилителя всегда существуют емкостные, индуктивные и гальванические паразитные связи, то на входе усилителя наряду с усиливаемым внешним сигналом присутствуют сигналы, проникшие во входные цепи через паразитную обратную связь, в том числе с выхода усилителя. Паразитную обратную связь можно также представить математической моделью $K_{ос}(\omega)e^{j\varphi_{ос}(\omega)}$. Обобщенная математическая модель усилителя с обратной связью представлена на рис. 5.9.

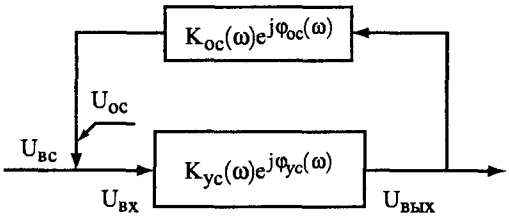



*Рис. 5.9.* Модель усилителя с обратной связью

Связь между выходом и входом усилителя описывается уравнением:

$$U_{вых} = (U_{вс} + U_{ос})\, K_{ус}(\omega)e^{j\varphi_{ус}(\omega)} = [U_{вс} + U_{вых}K_{ос}(\omega)e^{j\varphi_{ос}(\omega)}]K_{ус}(\omega)e^{j\varphi_{ус}(\omega)}.$$

После преобразования:

$$U_{вых} = U_{вс}\frac{K_{ус}(\omega)e^{j\varphi_{ус}(\omega)}}{1 - K_{ус}(\omega)K_{ос}(\omega)e^{j[\varphi_{ус}(\omega) + \varphi_{ос}(\omega)]}}.$$

Режим усиления переходит в режим генерации, когда выходной сигнал достигает максимального значения и поддерживается на этом уровне независимо от $U_{вх}$. Это условие выполняется при нулевом значении знаменателя указанного выше выражения. Следовательно, режим генерации возникает при $1 - K_{ус}(\omega)K_{ос}(\omega) \cdot e^{j[\varphi_{ус}(\omega) + \varphi_{ос}(\omega)]} \approx 0$.

Для этого необходимо выполнить два условия:

1) $K_{ос}(\omega) = 1/K_{ус}(\omega)$;
2) $\varphi_{ос}(\omega) = -\varphi_{ус}(\omega)$.

Первое условие определяет минимально необходимую для возникновения паразитной генерации величину коэффициента паразитной обратной связи. Чем выше коэффициент усиления усилителя, тем меньший коэффициент паразитной обратной связи создает предпосылки для возникновения генерации. Например, если $K_{ос} = 10$, то для возникновения генерации необходимо проникновение 0,1 части выходного сигнала на вход усилителя. Для усилителя с $K_{ус} = 100$ достаточно поступления на его вход 0,01 части выходного сигнала. Эта зависимость объясняет возможность паразитной генерации в логических элементах дискретной техники. Высокий коэффициент усиления логического элемента и высокая частота спектральных составляющих фронта дискретного сигнала создают благоприятные условия для возникновения паразитной генерации в логических элементах.

Второе условие предусматривает, что изменение фазы сигнала обратной связи должно быть противоположно величине фазового сдвига усилителя. Это означает, что фазы внешнего сигнала и сигнала обратной связи должны быть приблизительно равными. Обратная связь, при которой фаза сигнала на входе усилителя совпадает с фазой сигнала обратной связи, называется **положительной**, а когда фазы этих сигналов противоположные — **отрицательной**. Если положительная обратная связь способствует паразитной генерации, то отрицательная, наоборот, повышает стабильность работы усилителя, но за счет некоторого снижения напряжения на выходе усилителя. Поэтому в усилителях с высоким коэффициентом усиления для исключения паразитной генерации создают между каскадами отрицательную обратную связь, а также применяют комплекс мер по уменьшению паразитных связей. С этой целью при монтаже используют короткие экранированные провода, элементы входных и выходных цепей разносят на максимально возможное расстояние, экранируют трансформаторы усилителей, в цепи питания предварительных каскадов устанавливают RC-фильтры низких частот, усилительные каскады размещают в одну линию и др.

Опасность паразитной генерации состоит также в том, что она часто возникает на частотах выше рабочего диапазона и без специальных исследований не обнаруживается. Действительно, с ростом частоты обрабатываемых сигналов уменьшаются значения паразитных емкостных и индуктивных сопротивлений между каскадами. В результате этого увеличиваются $K_{oc}$ и сдвиг фазы сигналов, прошедших через паразитные связи. Поэтому возможность выполнения условий генерации в усилителе на частотах, превышающих верхнюю частоту рабочего диапазона частот усилителя, повышается. Хотя на этой частоте полезные сигналы на вход усилителя не подаются, но на его входе присутствуют сигналы, обусловленные тепловым шумом и проникшие через паразитную обратную связь. Любая шумовая реализация на входе усиливается усилителем и частично возвращается через паразитную обратную связь на его вход. При равенстве фаз величина суммарного сигнала на входе усилителя повышается, что приводит к росту сигнала на выходе усилителя. Следствием этого является увеличение сигнала $U_{oc}$ и дальнейшее увеличение сигнала на входе усилителя и т. д. Происходит лавинообразный процесс нарастания амплитуды сигнала на входе и выходе усилителя, завершаемый процессом непрерывной генерации на частоте $\omega_{рез}$. Поэтому не рекомендуется, например, применять в усилителях низкой частоты высокочастотные транзисторы, которые усиливают шумы с частотами выше верхней границы рабочего диапазона частот.

Паразитная генерация усилителя или логического элемента создает угрозу информации, если она записывается в информационные параметры паразитного колебания, т. е. происходит его модуляция информационными сигналами. Это явление возникает в случае, если цепи паразитного генератора содержат акустоэлектрические преобразователи или в них попадают опасные сигналы от других случайных акустоэлектрических преобразователей усилителя.

Люминофор электронно-лучевых трубок средств отображения под действием электронов излучает, кроме света, электромагнитное поле в широком диапазоне радиочастот с напряженностью, которая обеспечивает возможность перехвата сигналов на удалении в десятки метров. Учитывая, что сигналы управления электронным

лучом трубки подаются последовательно во времени, их побочные ВЧ-излучения создают серьезную угрозу для отображаемой на экране трубки информации.

Устройства компьютера, в которых распространяются сигналы в последовательном коде (мониторы, клавиатура, принтеры и другие), также представляют собой источники опасных сигналов. Замена монитора компьютера на электронно-лучевой трубке на жидкокристаллический монитор не устраняет проблему защиты информации, отображаемой на его экране. Хотя экран жидкокристаллического монитора не создает опасные излучения, но в устройстве управления значениями пикселей строки монитора присутствуют последовательные информационные сигналы. Спектр этих сигналов имеет широкий спектр в диапазоне сотен МГц. В результате их перехвата возможно восстановление изображения.

К **излучающим элементам ВЧ-навязывания** относятся радио- и механические элементы, которые обеспечивают модуляцию подводимых к ним внешних электрических и радиосигналов. К таким элементам относятся:

— нелинейные элементы, на которые одновременно поступают низкочастотный электрический сигнал с защищаемой информацией (опасный сигнал) и высокочастотный гармонический сигнал;

— токопроводящие механические конструкции, изменяющие свой размер и переотражающие внешнее электромагнитное поле.

Если на нелинейный элемент (диод, транзистор) подаются 2 сигнала: низкочастотный сигнал $u_c(t)$, в информационные параметры которых записана информация, и высокочастотный (сотни кГц —единицы МГц) гармонический сигнал $u_{вч}$ от внешнего генератора, то в токе через нелинейный элемент появятся высокочастотные составляющие, модулированные по амплитуде опасным сигналом. Действительно, ток, протекающий в нелинейном элементе в момент времени t, определяется суммой напряжений этих сигналов и сопротивлением цепи, в которой находится нелинейный элемент. В общем случае зависимость тока от напряжений сигналов имеет вид $i_{нэ} = f[u_c(t), u_{вч}(t)]$. Из-за нелинейности функции f(x) в токе возникают составляющие, представляющие различные комбинации ее аргументов. Действительно, если функция f(x)

описывается квадратичной зависимостью, то $i_{нэ} = k[u_c(t) + u_{вч}(t)]^2 = k[u_c(t)^2 + 2u_c(t)u_{вч}(t) + u(t)_{вч}{}^2]$, где k — нормирующий коэффициент. Если представить высокочастотный сигнал как $u_{вч}(t) = A_{вч}\sin\omega_{вч}t$, а опасный сигнал — в виде ряда Фурье

$$u_c(t) = C_0 + \sum_{k=1}^{n} C_k \sin(k\omega_{1\,0}t + \varphi_k),$$

то произведение

$$2u_c(t)u_{вч}(t) = 2A_{вч}C_0\sin\omega_{вч}t + A_{вч}\sum_{k=1}^{n} C_k\cos[(\omega_{вч} - k\omega_{1\,0})t - \varphi_k] -$$

$$- A_{вч}\sum_{k=1}^{n} C_k\cos[(\omega_{вч} + k\omega_{1\,0})t + \varphi_k].$$

Из этого выражения следует наличие в спектре тока высокочастотных гармоник опасного сигнала, несущих защищаемую информацию. Этот ток создает электромагнитное поле, мощность которого зависит не только от мощности сигналов, но и от соотношения длины его волны и длины цепи, по которой протекает ток. Такой вариант реализуется путем подачи внешнего высокочастотного электрического сигнала в телефонную проводную линию. Рассмотренный вариант реализуется путем подачи внешнего электрического сигнала в телефонную проводную линию.

Другим видом излучателя ВЧ-навязывания являются механические конструкции, способные изменять свой размер под действием акустической волны и переотражать внешнее электромагнитное поле. Такие конструкции, как правило, образуют замкнутую полость с токопроводящими поверхностями, одна из которых — тонкая и способна колебаться в соответствии с акустическим сигналом мембрана. При колебании мембраны изменяются геометрические размеры полости. Полость представляет собой колебательный контур, собственная частота которого определяется ее геометрическими размерами. При облучении конструкции электромагнитным полем с частотой колебания, равной собственной частоте контура, возникают резонансные явления и переотражается максимум энергии облучаемого поля. При колебаниях мембраны изменяются частота и напряженность переотраженного поля. После приема переотраженного поля из него можно выделить путем демодуляции электрический сигнал, соответствующий акустическому. Такой из-

лучатель ВЧ-навязывания по существу представляет собой пассивный акустоэлектрический преобразователь подводимой энергии.

Дальность распространения излучаемого ВЧ-электромагнитного поля зависит от его мощности, частоты колебания, величины затухания поля в среде и характера распространения поля.

Характер распространения электромагнитного поля в свободном пространстве описывается 4 уравнения Максвелла, приведенными им в 1873 г. в труде «Трактат об электричестве и магнетизме». Эти уравнения явились обобщением открытых ранее законов электрического и магнитного полей.

В соответствии с первым уравнением любое магнитное поле создается электрическими токами и изменением во времени электрического поля. Второе уравнение обобщает закон электромагнитной индукции, открытый Фарадеем в 1831 г., и указывает на то, что в результате изменения магнитного поля в любой среде появляется электрическое поле. Из третьего уравнения Максвелла следует, что поток вектора электрической индукции через любую замкнутую поверхность равен сумме зарядов в объеме, ограниченном этой поверхностью. Четвертое уравнение позволяет сделать вывод о том, что число силовых линий магнитного поля, входящих в среду некоторого объема, равно числу силовых линий, выходящих из этого объема. Это возможно при условии отсутствия в природе магнитных зарядов.

Из уравнений Максвелла также следует, что автономно (независимо) в природе могут существовать только постоянные электрические и магнитные поля. Поле, излучаемое зарядами и токами переменной частоты, является электромагнитным. В нем присутствуют электромагнитные и электрические компоненты, которые описываются взаимно перпендикулярными векторами. В зависимости от вида излучателя и расстояния от него до точки измерения характер изменения и соотношения между этими компонентами отличаются и изменяются. Характер распространения электромагнитного поля поддается точному математическому описанию для моделей излучателей в виде элементарных вибраторов. В качестве элементарного вибратора рассматривается модель излучателя, размеры которой существенно меньше длины волны излучаемого электромагнитного поля и расстояния от излучателя до точки

измерения. Для такой модели параметры излучения во всех точках принимаются равными. Различают элементарные электрический вибратор и магнитную рамку. Электрический вибратор возбуждается источником переменной электродвижущей силы (источником зарядов), магнитная рамка — протекающим по рамке током.

В реальных условиях, с учетом переотражения электромагнитных волн от многочисленных преград (зданий, стен помещений, автомобилей и т. д.), характер распространения столь сложен, что в общем случае не поддается строгому аналитическому описанию.

В зависимости от соотношения геометрических размеров источников излучений и расстояния от них до точки измерения поля различают **сосредоточенные и распределенные источники**. Сосредоточенные источники имеют размеры, существенно меньшие, чем расстояние от источника до точки наблюдения. К сосредоточенным источникам относится большинство радиоэлектронных средств и их узлов, а также головки громкоговорителей. Для распределенных источников их геометрические размеры соизмеримы или больше расстояния до них. Типовые распределенные источники электромагнитного излучения — провода кабелей линий связи.

## 5.4. Электромагнитные излучения сосредоточенных источников

Если сосредоточенный анизотропный излучатель представить в виде точки, от которой электромагнитные волны распространяются по всем направлениям с одинаковой энергией, то фронт волны образует сферу. Но по мере увеличения расстояния от излучателя кривизна сферы уменьшается и волна приближается к плоской электромагнитной волне.

По характеру распространения электромагнитной волны от сосредоточенного источника окружающего его пространство делят на 3 зоны: **ближнюю, переходную** и **дальнюю**. Условная граница между ними размыта. **Ближняя зона** располагается на удалении $r < \lambda/2\pi$ от источника. Пространство на расстояние $r > 3\lambda/2\pi$ рассматривается как **дальняя зона**. Размытая граница между ближней и дальней зонами называется **переходной зоной**.

В результате анализа уравнений Максвелла в разных зонах, можно сделать следующие выводы.

1. Если в качестве источника поля используется электрический вибратор, то в ближней зоне преобладает электрическое поле, напряженность E которого убывает с расстоянием в зависимости $1/r^3$. Магнитное поле электрического вибратора имеет меньшую напряженность, но убывающую медленнее — $H \sim 1/r^2$. При таком характере распространения электромагнитного поля электрического вибратора в переходной зоне значения напряженности электрической и магнитной составляющих сближаются, принимают одинаковые значения и убывают в дальней зоне обратно пропорционально r.

2. Если источником поля является магнитная рамка, то в ближней зоне $H >> E$. В этом случае характер распространения магнитной и электрической составляющих меняется на обратный: большая по величине напряженность H магнитного поля уменьшается в ближней зоне обратно пропорционально $r^3$, меньшая напряженность E электрического поля — обратно пропорциональна $r^2$. В переходной зоне зависимость напряженности электрического и магнитного полей от r изменяется от соотношения $1/r^2$ до соотношения $1/r$ в дальней зоне.

3. Величина связи между электрическими и магнитными компонентами электрического поля и равная $Z = E/H$ называется по аналогии с законом Ома **волновым сопротивлением**. Волновое сопротивление $Z_0$ свободного пространства (в вакууме) в дальней зоне равно 377 Ом. Так как напряженность электрического поля, излучаемого электрическим вибратором, в ближней зоне существенно выше напряженности магнитного поля, то в ней волновое сопротивление $Z >> Z_0$. Поэтому электрическое поле в ближней зоне называют также **высокоимпедансным**. В связи с тем что в ближней зоне напряженность магнитного поля, излучаемого магнитной рамкой, значительно больше напряженности электрического поля, в ней волновое сопротивление $Z << Z_0$. Такое поле называют **низкоимпедансным**.

4. В обобщенном виде характер электромагнитного поля и изменения волнового сопротивления в зависимости от расстояния ее источника иллюстрируется на рис. 5.10.

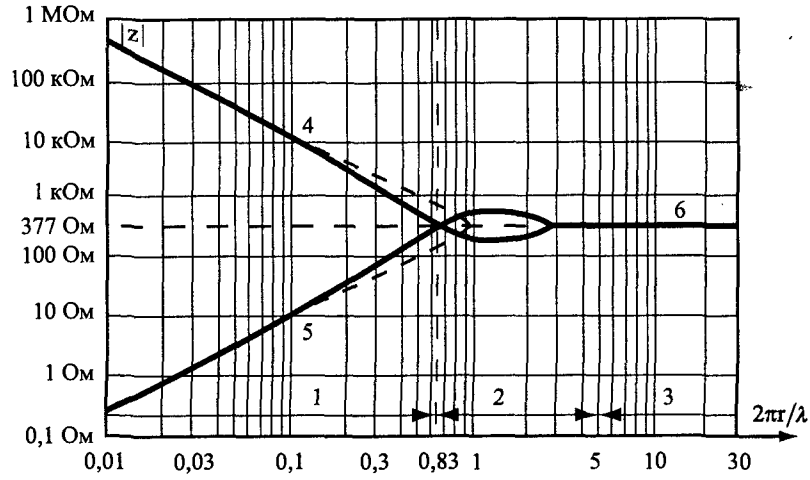



*Рис. 5.10.* Волновое сопротивление пространства электромагнитному полю

*Обозначения*: 1 — ближняя зона, 2 — переходная зона, 3 — дальняя зона, 4 — высокоомное электрическое поле, 5 — низкоомное магнитное поле, 6 — электромагнитное поле. Пунктиром на рисунке показана математическая зависимость, аппроксимирующая реальную.

На рисунке наглядно видно, что в зависимости от источника излучения для ближней зоны характерно преобладание электрического (с высоким волновым сопротивлением) или магнитного (с низким волновым сопротивлением) полей. С увеличением расстояния от штыревой антенны волновое сопротивление уменьшается со скоростью приблизительно 20 дБ/декада от больших значений (сотни кОм) до малых значений и на большом расстоянии асимптотически приближается к волновому сопротивлению вакуума. Волновое сопротивление рамочной антенны, наоборот, сначала увеличивается от долей Ома со скоростью 20 дБ/декада до сотен кОм и затем также асимптотически приближается к волновому сопротивлению вакуума. В переходной зоне наблюдаются колебания волнового сопротивления. В дальней зоне независимо от вида источника присутствует электромагнитное поле, волновое сопротивление которому в вакууме составляет 377 Ом.

Следовательно, при оценке уровней радиосигналов вблизи источников излучения необходимо учитывать существенно более сложный характер распространения электромагнитной волны по сравнению с традиционно рассматриваемым в дальней зоне.

## 5.5. Электромагнитные излучения распределенных источников

Основными распределенными источниками магнитного, электрического и электромагнитного полей являются симметричные и несимметричные кабели. Характер излучения полей для симметричных и несимметричных кабелей существенно различается.

К **несимметричным** относятся кабели, провода которых имеют разные электрические параметры или по проводникам протекают разные токи. Примеры несимметричного кабеля — коаксиальный телевизионный кабели и ленточные кабели для соединения устройств компьютера. В коаксиальном кабеле токи протекают по центральному проводу и экрану, имеющие различные электрические параметры. Проводники ленточных кабелей имеют одинаковые электрические параметры, но по информационным и корпусным проводникам протекают разные токи. Несимметричном кабель, по которому протекает электрический ток (рис. 5.11), образует магнитную рамку, напряженность излучения которого пропорциональна току и площади рамки.

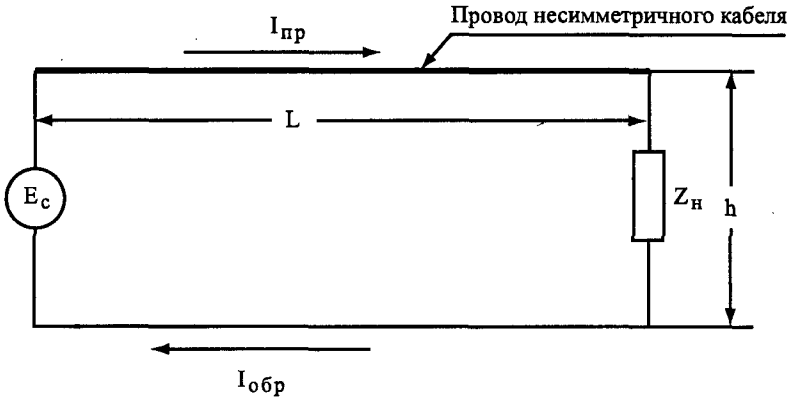



*Рис. 5.11.* Несимметричный кабель

Показанная на рисунке цепь образует магнитную рамку площадью $S_р = L \cdot h$. Чем больше площадь рамки и ток, протекающий в ней, тем выше уровень ее электромагнитного излучения.

**Симметричный кабель** состоит из четного количества проводов с одинаковыми электрическими и магнитными свойствами. По двум из них распространяется одинаковый по величине, но противоположный по фазе электрический ток. Токи в этих проводах создают магнитные поля одинаковой напряженности и противоположными по направлению магнитными силовыми линиями. В точке пространства, равноудаленном от обоих проводов, поля взаимно компенсируют друг друга и излучение отсутствует. Однако в точках пространства, находящихся на разном расстоянии от проводов, напряженность поля от более близкого провода будет превышать напряженность от более удаленного и полной компенсации противоположных по фазе полей не произойдет. Следовательно, напряженность поля симметричного кабеля может изменяться от 0 до максимального значения при измерении ее в точке, находящейся в плоскости проводов симметричного кабеля (рис. 5.12).

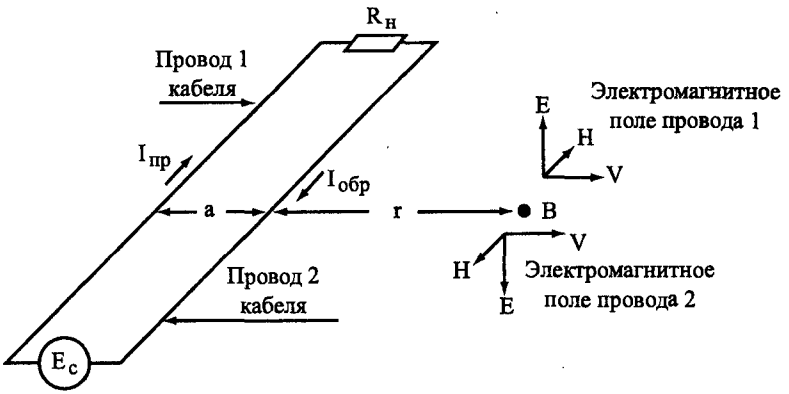



*Рис. 5.12.* Модель электромагнитного излучения симметричного кабеля

Напряженность остаточного магнитного поля из-за асимметричности расположения проводов (без учета магнитного поля Земли и других его источников) для этой модели определяется по формуле:

$$H_r = \frac{Ia}{2r\pi(r + a)},$$

где I — ток в проводах; a — расстояние между параллельными проводами; r — расстояние от точки измерения напряженности В до ближайшего провода.

Так как r >> a, то $H_r \approx \frac{Ia}{2\pi r^2}$. Следовательно, мощность излучения поля симметричным кабелем пропорциональна расстоянию между проводами и обратно пропорциональна квадрату расстояния от них.

Асимметричность расположения проводов симметричного кабеля по отношению к поверхности Земли или других токопроводящих поверхностей вызывает неравенство паразитных связей между проводниками этих кабелей и другими токопроводящими поверхностями. В результате этого в них возникают некомпенсируемые токи, которые создают дополнительные побочные электромагнитные излучения. Физические явления, приводящие к асимметричности токов в земле, иллюстрируются моделью на рис. 5.13.

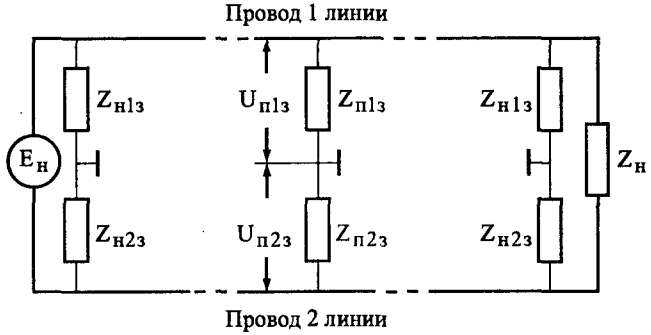



*Рис. 5.13.* Цепь Пикара

Приведенная на рисунке цепь называется цепью Пикара, сопротивления $Z_{и1з}$, $Z_{и2з}$, $Z_{п1з}$, $Z_{п2з}$, $Z_{и1з}$ и $Z_{и2з}$ которой обозначают сопротивления, возникающие за счет паразитных связей между ис-

точником, проводами линии, нагрузкой и землей соответственно. При наличии этих сопротивлений кроме основной, функциональной цепи возникает множество дополнительных цепей между источником сигналов и нагрузкой с участками по земле. В силу асимметричности расположения проводов относительно земли $Z_{п1з} \neq Z_{и2з}$, $Z_{п1з} \neq Z_{п2з}$ и $Z_{п1з} \neq Z_{и2з}$. Из неравенства указанных сопротивлений токи, протекающие по проводам 1 и 2, через рассматриваемые сопротивления, а также по земле в противоположных направлениях не равны. В результате этого возникает магнитная рамка, излучающая электромагнитное поле с преобладанием магнитной компоненты в ближней зоне.

Таким образом, распределенные источники излучений создают электромагнитные излучения несимметричных и симметричных кабелей. Несимметричный кабель образует магнитную рамку, образованную информационным проводом и землей. Излучения симметричного кабеля создаются за счет асимметрии кабеля относительно точки измерения и земли.

## 5.6. Утечка информации по цепям электропитания

К цепям, имеющим выход за пределы контролируемой зоны и в которые могут проникнуть опасные сигналы через паразитные связи любых видов, относятся, прежде всего, цепи электропитания. Поэтому предотвращение утечки информации по этим цепям является одной из задач инженерно-технической защиты информации.

Цепи электропитания обеспечивают передачу электрической энергии в виде переменного электрического тока напряжением 380/220 В и частотой 50 Гц от внешних источников (подстанций) подавляющему большинству устанавливаемых в помещениях радио- и электрических приборов (технических средств и систем — ТСС). Соединение источника и приемника производят при помощи трех или четырех проводов. При трехпроводной линии передачи источники могут быть соединены как треугольником, так и звездой (рис. 5.14).

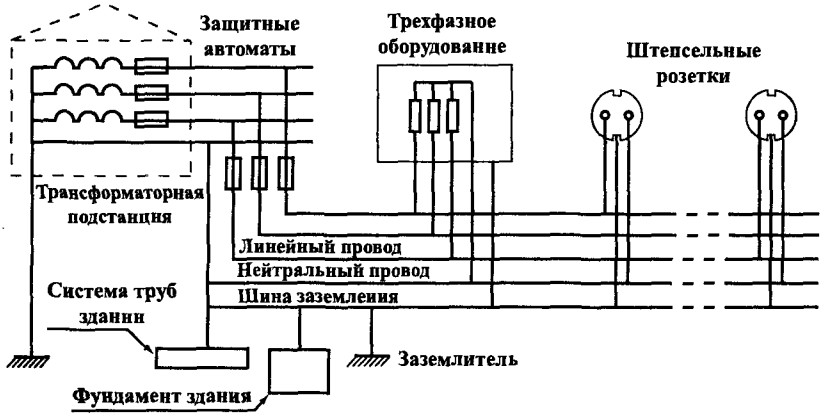



*Рис. 5.14.* Схема цепей электропитания здания

В последнем случае точка соединения концов обмоток трансформатора (нейтральный провод — нейтрал) остается неподключенной и схема подключения не имеет нейтрального провода. Чаще используемую четырехпроводную линию передачи электроэнергии применяют при соединении фаз источника и приемника звездой. Один из проводов соединяет точки нейтралей и заземляется (рис. 5.14). Напряжение каждой фазы относительно нейтрального провода (фазовое напряжение) при соединении звездой составляет 220 В, линейное напряжение (между фазами) больше — 380 В. Трехфазное напряжение применяется для электропитания в основном мощных электродвигателей различных технических средств, однофазное напряжение 220 В — для электропитания радиоэлектронных средств и бытовых маломощных электрических приборов (ламп освещения, вентиляторов, холодильников, электронагревательных приборов и др.).

В качестве первичных источников электропитания ТСС используются трансформаторные подстанции (ТПС) типа ТП 6–10/04 кВ или другие, понижающие трехфазное напряжение 6–10 кВ от центрального распределительного пункта (ЦРП) или главной понизительной подстанции (ГПП) до трехфазного напряжения 380 В. К потребителям электроэнергия от трансформаторной подстанции подается, как правило, по радиальной схеме, в соответствии с которой каждый потребитель или их группа питается по отдельной

линии от соответствующего коммутационного узла. Линии передачи представляют собой, как правило, четырехжильные силовые кабели.

Так как цепи электропитания выходят за пределы охраняемой зоны, то распространение по ним опасных сигналов создает угрозу безопасности защищаемой информации. Существуют, по крайней мере, 4 причины появления опасных сигналов в цепях электропитания.

Первой причиной является наведение в них ЭДС полями НЧ и ВЧ побочных излучений ОТСС.

Вторая причина обусловлена модуляцией тока электропитания токами радиоэлектронного средства (РЭС). Иллюстрирующая эту причину модель представлена на рис. 5.15.

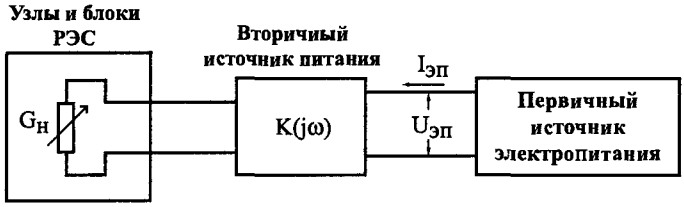



*Рис. 5.15.* Модель цепи электропитания

Источником электропитания радиоэлектронного средства является блок питания, который можно представить в виде передаточной функции K(jω). Нагрузкой вторичного источника электропитания являются узлы и блоки РЭС. Эту нагрузку можно представить в виде сопротивления или проводимости $G_н(t)$. Величина проводимости нагрузки меняется в соответствии с характером изменения величины обрабатываемого полезного сигнала S(t), т. е. $G_н(t) \equiv S(t)$. Ток в цепи электропитания блока равен величине $I_{эп}(t) = U_{эп}(t)K(j\omega)G_н(\omega)$, где $U_{эп}(t) = U_{оп}\sin\omega_п t$ — напряжение электропитания РЭС от первичного источника тока с номинальным напряжением $U_{ол} = 220$ В и частотой $f_п = 50$ Гц. Если полезный сигнал $S(t) = U_c\sin\omega_c t$, то проводимость $G_н = G_{он}\sin\omega_c t$, где $G_{он}$ — среднее значение проводимости при среднем значении полезного сигнала. Для упрощения примем, что на частотах полезного сигнала $K(j\omega) \approx 1$. В этом случае ток в цепи электропитания можно представить в виде выражения $I_c(t) = U_{оп}G_{он}\sin\omega_c t \cdot \sin\omega_п t = 0{,}5U_{оп}G_{он}[\cos(\omega_c - \omega_п) - \cos(\omega_c + \omega_п)]$. Из

его анализа следует, что ток в цепи электропитания содержит составляющие с частотами полезного сигнала, которые можно выделить и с которых можно снять информацию.

Типовой вторичный источник питания (блок питания) состоит из следующих последовательно соединяемых узлов:

- сетевого трансформатора с коэффициентом трансформации n;
- выпрямителя;
- фильтра блока питания;
- стабилизатора;
- устройства для защиты блока питания от короткого замыкания.

Трансформатор преобразует напряжение 220 В в напряжение питания узла (блока) радиоэлектронного средства. Для получения постоянного напряжения переменный ток выпрямляется и с целью уменьшения пульсаций фильтруется. Параметры фильтра определяются из условия обеспечения допустимого коэффициента пульсаций напряжения питания порядка 1–2% выходных каскадов РЭС, токи в которых составляют большую часть токов через эквивалентную нагрузку с проводимостью $G_{н}$.

Каждый из узлов блока питания оказывает определенное влияние на К(ω). Наибольшие искажения вносят фильтр питания и стабилизатор, которые можно представить в виде фильтра низкой частоты с максимальной частотой пропускания около 30 Гц. Следовательно, типовой вторичный источник питания пропускает от РЭС в цепи электропитания сигналы в диапазоне 0–30 Гц. Если в радиоэлектронном средстве осуществляется обработка (усиление) речевых сигналов, то вторичный источник питания вырезает из его спектра участок шириной до 30 Гц и подавляет спектральные составляющие большей частоты. Учитывая, что спектр речевого сигнала лежит в диапазоне сотен Гц-единиц кГц, вторичный источник питания не пропускает спектральные составляющие речевого сигнала, но пропускает его огибающую. Огибающая речевого сигнала имеет полосу до 60–100 Гц, но его основная энергия сосредоточена в полосе до 30 Гц. Попадание в цепи электропитания огибающей речевого сигнала позволяет при ее перехвате понять смысл сообщения.

В соответствии с третьей причиной опасный сигнал может попасть в цепи электропитания через паразитные связи элементов схемы и элементов блока питания. Например, между первичной и вторичной обмотками сетевого (силового) трансформатора существуют индуктивная и емкостная паразитные связи, через которые опасные сигналы могут поступать от узлов и блоков РЭС в цепи электропитания без существенного ослабления его сердечником трансформатора.

Четвертая причина вызвана процессами в импульсных блоках питания РЭС, которые применяются вместо традиционных блоков питания с силовыми трансформаторами для частоты 50 Гц. Силовой трансформатор низкой частоты традиционного блока питания имеет большие габариты и вес, которые сдерживают миниатюризацию бытовой и профессиональной радиоаппаратуры. Также велики размеры и вес элементов фильтров (индуктивностей и конденсаторов) выпрямителя блока питания при преобразовании напряжений на частоте 50 Гц. С повышением частоты питающего напряжения уменьшаются габариты и вес блока питания. Поэтому для радиоаппаратуры, устанавливаемой, например, на борту самолетов, используются источники электропитания на более высокой частоте 400 Гц.

В современных импульсных блоках питания напряжение 220 В от первичного источника коммутируется электронным ключом, управляемым импульсным генератором с частотой повторения импульсов порядка 100 кГц. Высокочастотное питающее напряжение подается на импульсный трансформатор, выпрямитель, стабилизатор и фильтр блока питания с существенно меньшими габаритами и весом.

Однако высокочастотный ток, протекающий через ключ, имеет сложную форму и, соответственно, широкий спектр. Этот спектр может содержать составляющие, образующиеся в результате комбинаций сигналов импульсного генератора и информационных сигналов, проникающих через паразитные связи из узлов РЭС в элементы блока питания. Высокая частота этих опасных сигналов обеспечивает условия для их излучения в эфир с уровнем, достаточным для обнаружения и приема на удалении нескольких десятков метров.

## 5.7. Утечка информации по цепям заземления

Так как цепи заземления выходят за пределы помещения и здания, то распространяющиеся по ним опасные сигналы создают угрозы содержащейся в них информации. Цепи заземления в общем случае создаются для выполнения следующих функций:

- исключение возможности поражения электрическим током персонала, обслуживающего технические средства (защитная функция);
- установление опорного (общего) «нуля» для измерений уровней измеряемых сигналов (базовая функция);
- экранирование электрического поля (экранирующая функция);
- обеспечение путей для протекания возвратных (обратных) питающих и сигнальных токов (возвратная функция).

При заземлении используются два понятия: «земля» и «масса». Под массой понимаются схемотехнические конструкции (шина, провод опорного потенциала, корпус, нулевая точка, нейтрал), по отношению к которым измеряются потенциалы сигналов схемы. «Масса» и «земля», как правило, но не всегда, гальванически связаны друг с другом, а их потенциалы могут отличаться. Потенциал земли, так же как уровень океана, принимается за нулевой. Независимо от выполняемой функции ее эффективность тем выше, чем меньше сопротивление цепи заземления, включающей шину заземления и заземлитель.

Опасные сигналы в цепях заземления возникают по двум причинам:

- наведение в цепях заземления ЭДС полями побочных электромагнитных излучений;
- протекание тока заземления по контуру заземления.

Образование контура заземления иллюстрируется рис. 5.16.

На нем показаны паразитные емкостные связи $C_{п1}$ и $C_{п2}$. Емкость $C_{п2}$ соответствует величине паразитной емкостной связи между элементами схемы и землей, а емкость $C_{п1}$ — величине емкостной паразитной связи между элементами схемы, в которой циркулируют сигналы $E_c$ с защищаемой информацией, и массой (корпусом).

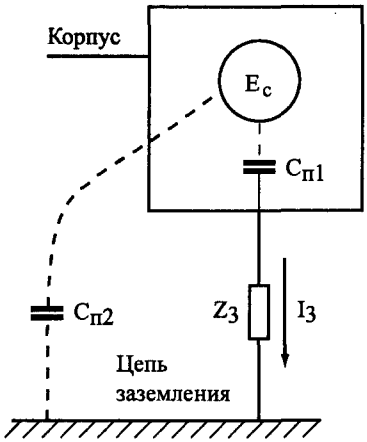



*Рис. 5.16.* Модель цепи заземления

Цепь заземления корпуса имеет сопротивление $Z_з$. Как видно из рис. 5.15, паразитные емкостные связи, цепь заземления, земля и эквивалентный источник образуют замкнутую цепь, ток в которой равен величине

$$I_з = \frac{E_c}{Z_c + Z_з},$$

где $Z_c = (C_{п1} + C_{п2})/j\omega C_{п1}C_{п2}$ — суммарное сопротивление двух последовательно соединенных емкостей $C_{п1}$ и $C_{п2}$.

Так как $C_{п1} >> C_{п2}$, то $Z_c \approx 1/j\omega C_{п2}$. Для низких частот $Z_c >> Z_з$ и $I_з \approx j\omega E_c C_{п2}$. Следовательно, чем выше частота сигнала, тем больше ток заземления.

Опасный сигнал может быть «снят» с цепи заземления индуктивным способом или с сопротивления, включенного последовательно в эту цепь. Так как обычно к одной шине заземления подключается несколько радиоэлектронных средств, то протекающие по ней токи представляют собой смесь токов разных источников. Поэтому выделение в этой смеси опасных сигналов из определенного помещения возможно в принципе, но связано с выполнением ряда условий, в том числе с обеспечением отношения сигнал/помеха, необходимым для выделения информации с требуемым качес-

твом. Помехи представляют собой не только тепловые шумы, но и сигналы других радиоэлектронных средств.

### Вопросы для самопроверки

1. Виды побочных электромагнитных излучений и наводок.
2. Чем отличаются активные акустоэлектрические преобразователи от пассивных?
3. Какие угрозы создают случайные акустоэлектрические преобразователи?
4. Виды паразитных связей. Физические явления, вызывающие емкостные и индуктивные паразитные связи.
5. Когда возникает паразитная гальваническая связь?
6. Физический смысл действующей высоты и действующей длины антенны.
7. Источники побочных низкочастотных и высокочастотных излучений.
8. Условия возникновения паразитных колебаний в усилителе.
9. Характер распространения электромагнитной волны в ближней зоне.
10. Характер излучения электромагнитного поля симметричного и несимметричного кабелей.
11. Причины, вызывающие появление опасных сигналов в цепях электропитания.
12. Физические процессы, приводящие к утечке информации по цепям заземления.

# Глава 6. Технические каналы утечки информации

## 6.1. Особенности утечки информации

Под **утечкой информации** понимается несанкционированный перенос информации от ее источника к злоумышленнику. Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации и т. д. Утечка информации возможна путем ее разглашения людьми, утерей ими носителей с информацией, переносом информации с помощью полей, потоков элементарных частиц, веществ в газообразном, жидком или твердом виде. Например, желание сотрудников поделиться последними новостями о работе с родными или близкими создает предпосылки для утечки конфиденциальной информации. Переносчиками информации могут быть любые ее носители.

Часто под утечкой понимают процесс вроде вытекания воды из неисправного крана. Например, утечку иногда определяют как несанкционированное распространение носителя с защищаемой информацией за пределы контролируемой зоны. Такой подход представляется неверным, так как для информации не выполняется закон сохранения материи. Средства массовой информации миллионными экземплярами тиражируют сведения и при этом с их источником ничего не происходит.

Утечка информации по сравнению с утечкой (хищением) материальных объектов имеет ряд особенностей, которые надо учитывать при организации защиты информации:

- при утечке информации не выполняются законы сохранения материи, вследствие чего утечка не может быть обнаружена в результате уменьшения количества информации источника;
- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;
- при утечке информации вследствие расширения круга ее потребителей цена информации уменьшается.

Первая особенность существенно усложняет своевременное обнаружение утечки информации. При утечке материальных объектов достаточно провести ревизию их наличия для обнаружения утечки объектов в результате, например, хищения. При утечке информации могут отсутствовать явные признаки ее хищения: документы в наличии, оттиски печатей на сейфе не нарушены, следов проникновения в помещение посторонних лиц нет. Однако появление косвенных признаков (внезапный выброс на рынок конкурентного товара с идентичными потребительскими свойствами, срыв по непонятным причинам выполнения договора и др.) вынуждает в качестве причины этих событий рассматривать утечку информации. Из-за существенного запаздывания проявляющихся признаков по отношению ко времени утечки информации задача хотя бы частичной нейтрализации ее последствий становится весьма проблематичной.

Вторая особенность имеет существенное значение для безопасности информации, так как сами по себе факты утери документа, разглашения сведений, распространения носителей за пределы контролируемой зоны и другие действия далеко не всегда приводят к утечке информации. Например, если конфиденциальный разговор во время совещания в кабинете руководителя организации слышен в приемной из-за неплотно закрытой двери, а в приемной нет посторонних людей, то утечки информации нет, хотя носитель информации (акустическая волна) выходит за пределы контролируемой зоны — кабинета. Только в том случае, когда в приемной будет находиться сотрудник организации или посетитель, который воспользуется информацией из услышанного разговора в личных или иных целях или поделится ею с другими заинтересованными в ней людьми, происходит утечка информации из кабинета руководителя.

В общем случае можно говорить об утечке информации как факте нарушения ее безопасности только в том случае, если она попадает к злоумышленнику независимо от того, знает или не знает об этом владелец информации. Если по какой-то причине на этом пути передачи информации происходит разрыв в цепочке, то информация исчезает вместе с ее носителем, а утечки информации не происходит.

Следовательно, под утечкой следует понимать не процесс распространения носителя, а вариант распространения, заканчивающийся попаданием информации к злоумышленнику. Выход же носителя за пределы заданной области создает предпосылки для утечки информации и повышает угрозу ее безопасности. Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Возможность утечки информации характеризуется **риском утечки**, а целенаправленная деятельность по изменению возможности утечки называется **управлением риском**.

Часто хищение и утечку информации рассматривают как автономные процессы. Если под хищением понимать умышленное присвоение чужой собственности без разрешения ее законного владельца, то несанкционированное получение информации в результате ее утечки представляет собой один из способов ее хищения. Действительно, если человек на государственной земле находит клад, слиток из драгоценных металлов или драгоценный камень, которые по закону являются собственностью государства, то он обязан их сдать соответствующему государственному органу. В противном случае его действия классифицируются как хищение и он может быть привлечен к ответственности. Аналогичная ситуация с утечкой информации. Когда злоумышленник находит утерянный документ с грифом «секретно» и сознательно, понимая о наносимом владельцу информации ущербе, продает его зарубежной спецслужбе, то он может быть привлечен к уголовной ответственности за хищение государственной тайны.

## 6.2. Типовая структура и виды технических каналов утечки информации

Физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику образует **канал утечки информации**. В зависимости от вида носителя информации каналы ее утечки различаются структурой. Если распространение информации происходит с помощью

технических средств, то соответствующий канал называется **техническим каналом утечки информации**. Обобщенная структура типового технического канала утечки приведена на рис. 6.1.

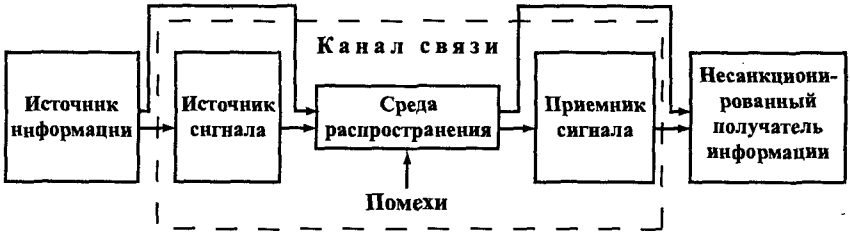



*Рис. 6.1.* Структура технического канала утечки информации

Как следует из этого рисунка, переносимая информация может содержаться как на носителях, являющихся одновременно ее источниками, так и носителях-переносчиках, на которые она переписывается с источников. Например, отходы делопроизводства, являющиеся источниками информации, могут переноситься людьми или стихийными силами в пространстве от места нахождения источника до злоумышленника, образуя канал утечки информации. Поэтому канал утечки информации на макротелах содержит источник информации, среду распространения носителя и несанкционированный получатель. Информация, переносимая динамическими носителями в виде полей (акустических и электромагнитных) и электрического тока, предварительно переписывается в источнике сигналов в их информационные параметры. В связи источник сигнала, среда ее распространения и приемник сигнала образуют в совокупности **канал связи**. Задача канала связи заключается в передаче входной информации санкционированному получателю с минимальными искажениями, временными, энергетическими и другими затратами.

Канал утечки информации на носителях в виде полей и элементарных частиц содержит те же элементы, что и канал связи. Отличие между ними условное — в зависимости от получателя информации. У канала связи получатель информации санкционированный, у канала утечки — несанкционированный. Например, злоумышленник, внедряя закладное устройство, создает канал связи, который по отношению к ее источнику является каналом утечки

информации. Следует также отметить, что наличие канала утечки является необходимым, но недостаточным условием утечки информации. При отсутствии источника информации и ее получателя утечки информации нет. По аналогии, например, канал телефонной связи существует постоянно, но передача информации происходит тогда, когда абоненты на концах канала связи начинают разговаривать.

На вход канала связи поступает информация в виде первичного сигнала или сам источник может быть источником информации. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источников сигналов могут быть:

- объект наблюдения, отражающий электромагнитные волны, в том числе свет;
- объект наблюдения, излучающий собственные электромагнитные волны в оптическом и радиодиапазонах, вызванные тепловым движением электронов;
- движущиеся механизмы и машины, создающие акустические сигналы;
- передатчики функциональных каналов связи;
- ретрансляторы, например закладные устройства;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- радиоактивные материалы.

Как следует из этого перечня, большинство источников сигналов являются одновременно источниками информации о видовых, сигнальных или вещественных признаках. Только в случае, когда передается семантическая информация, она поступает на вход источника сигнала на носителе в виде первичного сигнала.

Указанные на рисунке стрелками пути входа и выхода информации обозначают вход и выход первичных сигналов с информацией. Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, кодов, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствую-

щий среде распространения. В общем случае источник сигнала выполняет следующие функции:

- создает (генерирует) поле (акустическое, электромагнитное) или электрический ток, которые переносят информацию;
- производит запись информации на носитель (модуляцию информационных параметров носителя);
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Запись информации производится путем изменения параметров носителя в соответствии с уровнем первичного сигнала, поступающего на вход. Если носителями информации являются субъекты и материальные тела (макрочастицы), то передатчик соответствует первоначальному смыслу этого слова — передавать или переносить, т. е. выполняет функцию носителя. В случае когда информацию переносят сигналы (поля, электрический ток и элементарные частицы), то передатчики являются источниками сигналов.

**Среда распространения носителя** — часть пространства, в которой перемещается носитель от источника сигнала к его приемнику. Среда распространения может быть в виде свободного пространства и направляющих линий. В качестве направляющих линий используются электрические провода различной конфигурации, волноводы, волоконно-оптические кабели, звукопроводы и другие конструкции. Их пространственное положение определяет маршрут движения носителя в пространстве. При передаче информации по направляющим линиям функциональных каналов связи обеспечиваются меньшие потери энергии носителя на бесполезное облучение пространства и большая безопасность информации, чем при распространении носителей в свободном пространстве. Однако при этом резко возрастают затраты на создание и эксплуатацию таких каналов связи.

**Приемник сигнала** выполняет функцию, обратную функции передатчика. Он производит:

- выбор (селекцию) носителя с нужной получателю информацией;

- усиление принятого сигнала-носителя до значений, обеспечивающих съем информации;
- съем информации с носителя (демодуляцию, декодирование);
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление первичных сигналов до значений, необходимых для их восприятия человеком и техническим устройством.

Если получатель информации человек, то информация с выхода приемника должна быть представлена на языке общения людей. Если техническое устройство, то форма представления информации должна быть понятна этому устройству. Например, если получатель ЭВМ, то с выхода приемника на ЭВМ подается двоичная последовательность в кодах, например, таблицы ASCII DOS, КОИ8, Windows и др.

В среде могут распространяться носители с другой информацией, которые по отношению к носителю с рассматриваемой информацией являются **помехами**. Чем ближе признаки носителя с защищаемой информацией и помех, тем сложнее приемнику их различить и тем сильнее влияние помех на информацию. Например, если частоты помехи и радиосигнала отличаются на величину более полосы пропускания приемника, то помеха будет подавлена селективными цепями приемника. Если их частоты пересекаются, то после демодуляции помеха наложится на сигнал, что приведет к изменению информационных параметров сигнала, вплоть до полного разрушения информации. Постоянно растущее количество сигналов в радиодиапазоне породило достаточно серьезную проблему их электромагнитной совместимости. Для санкционированных источников эта проблема решается организационными мерами: законодательным распределением шкалы радиодиапазона между различными источниками и контролем за дисциплиной связи. Но эти меры плохо работают применительно к источникам помех. Например, рост парка автомобилей в городе повышает насыщенность эфира помехами от их систем зажигания, которые полностью не подавляются установленными в них фильтрами.

Классификация каналов утечки информации по различным классификационным признакам дана на рис. 6.2.

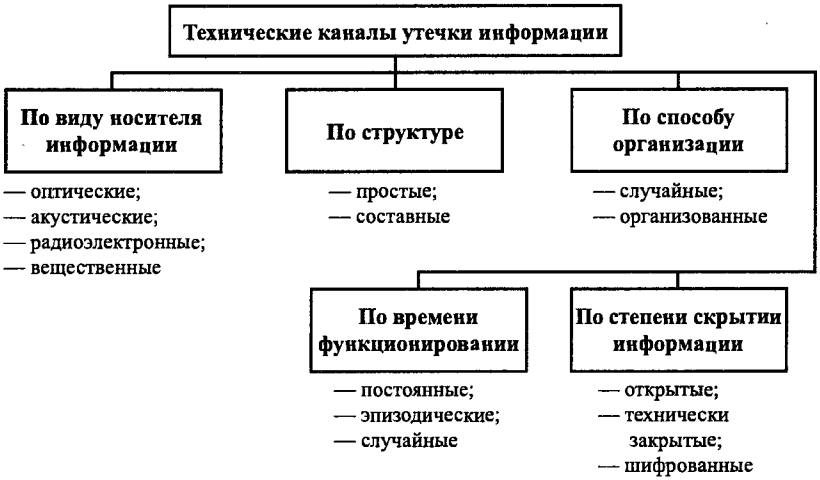



*Рис. 6.2.* Классификация технических каналов утечки информации

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя. По этому признаку они делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- вещественные.

В литературе встречаются иные названия каналов утечки информации. В принципе возможны любые названия, если они только соответствуют одному признаку классификации, обеспечивают полноту и непересекаемость элементов классификации.

Носителем информации в **оптическом канале** является электромагнитное поле (фотоны) в диапазоне 0,46–0,76 мкм (видимый свет) и 0,76–13 мкм (инфракрасные излучения).

В **радиоэлектронном канале** утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон колебаний носителя этого вида чрезвычайно велик: от звукового диапазона до десятков ГГц.

В соответствии с видами носителей информации радиоэлектронный канал целесообразно разделить на 2 подвида: **электромагнитный канал**, носителями информации в котором являются электрическое, магнитное и электромагнитное поля, и **электрический канал**, носитель информации в котором — электрический ток.

Носителями информации в **акустическом канале** являются упругие акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц–20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В **вещественном канале** утечка информации производится путем несанкционированного распространения носителей с защищаемой информацией в виде вещества, прежде всего выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ и др. Демаскирующие вещества в виде твердых, жидких и газообразных отходов или промежуточных продуктов позволяют определить состав, структуру и свойства новых материалов или восстановить технологию их получения. К утечке по этому каналу отнесено несанкционированное распространение продуктов распада радиоактивных веществ, обнаружение и распознавание которых злоумышленником обеспечивают возможность определения наличия и признаков радиоактивных веществ.

Когда речь идет о распространении за пределы организации отходов производства, следует отличать технический канал утечки от агентурного, в рамках которого вынос носителя с информацией производится проникшим к источнику злоумышленником, завербованным сотрудником организации или сотрудником, стремящимся продать информации любому ее покупателю. Граница между агентурным и каналом утечки достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом вещественном канале носители вывозятся из организации с целью освобождения ее от отходов или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие выбрасываемые трубами газообразные отходы, или водные потоки рек или водоемов,

куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от ее утечки.

Технический канал утечки информации, состоящий из передатчика, среды распространения и приемника, является **простым** или **одноканальным**.

Однако возможны варианты, когда утечка информации происходит более сложным путем — по нескольким последовательным или параллельным каналам. В этом случае канал можно назвать **составным**. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому — путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка — среда распространения — радиоприемник) каналов. Такие каналы корректно назвать **акусто-оптическим** и **акусто-радиоэлектронным** соответственно. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно разместить ретранслятор слабого сигнала закладного устройства в портфеле, сдаваемый якобы на хранение в камеру хранения закрытого предприятия, а принимать и регистрировать более мощный сигнал ретранслятора на удалении в несколько километров в безопасном месте. Такой составной канал называется **акусто-радиоэлектронный-радиоэлектронный**.

По частоте проявления каналы делятся на **постоянные** и **эпизодические**. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете ис-

точника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Регулярность получения информации через такой канал делает его весьма ценным. Поэтому разведка дорожит регулярным источником информации и защищает его от контрразведки. К эпизодическим каналам относятся каналы, утечка информации в которых имеет кратковременный, часто случайный характер.

По способу создания каналы утечки могут быть специально **организованные** и **случайные**. Организованные каналы создаются злоумышленником для регулярного добывания информации. Например, для подслушивания на большом расстоянии от источника речевой информации организуется канал утечки из помещения путем размещения в нем закладного устройства. Характеристики (частота излучения, вид модуляции, мощность передатчика и др.) этого канала известны злоумышленнику. Эти знания позволяют ему непрерывно или в определенное время прослушивать все разговоры, ведущиеся в помещении.

Побочные электромагнитные излучения и наводки создают предпосылки для образования случайных каналов утечки информации, параметры которых априори злоумышленнику не известны. Если ему удастся настроить свой приемник на частоту побочного излучения, то возникает случайный канал утечки информации. Такой канал может быть весьма информативным, но случайный характер его образования и времени работы (когда включено излучающее техническое средство) снижает его полезность для злоумышленника.

По техническому каналу утечки информация может передаваться не только в открытом виде, она может быть и закрытой. С целью повышения скрытности сигнал на выходе перспективных закладных устройств закрывается, а канал утечки, использующий эти устройства, является **технически закрытым**. При перехвате функциональных каналов связи, по которым передается шифрованная информация, образуется шифрованный канал утечки информации.

Возможности передачи информации по техническим каналам зависит от многих факторов: энергии сигнала, степени его ослабления в среде распространения, чувствительности и разрешающей

способности приемника злоумышленника, уровня помех в канале и др.

## 6.3. Основные показатели технических каналов утечки информации

Технический канал утечки информации характеризуется показателями, которые позволяют оценить риск утечки. Такими показателями являются:

— пропускная способность технического канала утечки;
— длина технического канала утечки информации;
— относительная информативность технического канала утечки информации.

По аналогии с каналом связи интегральные возможности технического канала утечки по передаче информации оцениваются его **пропускной способностью**. Предельная пропускная способность канала связи в битах в секунду определяется по формуле [13]:

$$C = \Delta F \log_2 (1 + P_c/P_п),$$

где $\Delta F$ — ширина полосы пропускания канала связи в Гц; $P_c$ и $P_п$ — мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Из нее следует, что пропускная способность тем больше, чем шире полоса пропускания частот канала и больше отношение сигнал/шум на входе приемника канала связи.

Так как пропускная способность канала связи зависит от его полосы пропускания и отношения сигнал/шум, то каналы можно разделить на **узкополосные** и **широкополосные**, с **низкой** и **высокой энергетикой** сигнала. Наибольшую пропускную способность имеет оптический канал связи, наименьшую — акустический. Радиоэлектронные каналы связи по ширине полосы частот пропускания делятся на узкополосные и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300–3400 Гц и относится к узкополосным, а шириной 8 МГц для передачи телевизионных сигналов — к широкополосным. Если ширина спектра сигнала $\Delta F_c$, содержащего информацию, равна полосе пропускания частот канала $\Delta F_к$, то передача информации про-

исходит в реальном масштабе времени. Когда $\Delta F_c > \Delta F_к$, информация искажается и частично теряется (рис. 6.3).

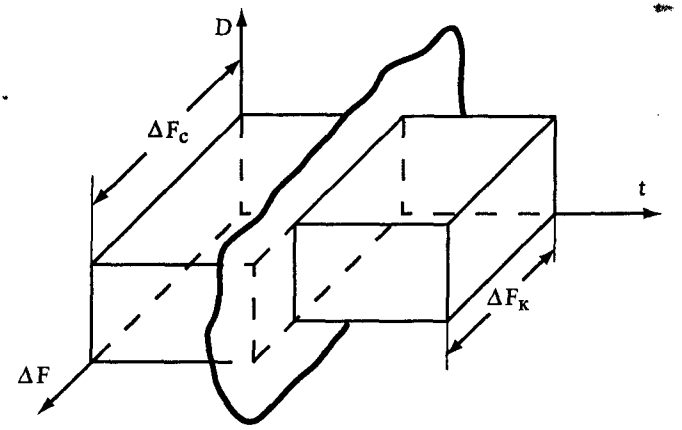



*Рис. 6.3.* Графическое представление ограничения частоты сигнала каналом утечки

Для исключения потери информации на входе канала связи применяется буферное запоминающее устройство, на вход которого поступает с определенной скоростью информация и с которого информация считывается со скоростью, обеспечивающей согласование ширины спектра сигнала с шириной полосы пропускания частот канала. При этом время передачи увеличивается, т. е. режим реального времени не обеспечивается. Если $\Delta F_c < \Delta F_к$, то спектр сигнала не урезается, но в более широкополосном канале увеличивается уровень помех. В результате этого уменьшается отношение сигнал/помеха, что также приводит к снижению пропускной способности канала связи.

Пропускная способность составного канала (состоящего из нескольких последовательно соединенных простых каналов) определяется пропускной способностью простого канала, имеющего наименьшие значения. Например, составной канал наблюдения объектов с космического аппарата включает широкополосный оптический канал «наземный объект — фотоаппарат КА» и менее широкополосный радиоэлектронный канал «сброса» изображения с КА получателю. Для передачи полученного при фотографирова-

нии объема видеоинформации изображения на пленке считывается с меньшей скоростью, но в течение более длительного времени. В общем случае наибольшую пропускную способность имеет оптический канал утечки информации, так как его полоса пропускания существенно выше полосы пропускания любого другого канала. Наименьшей пропускной способностью обладает акустический канал утечки информации.

Другим показателем, который широко применяется для оценки возможностей канала утечки, является его длина. **Длина технического канала** утечки информации оценивается расстоянием от источника сигнала канала до его приемника при условии обеспечения при приеме допустимого качества информации. Длина канала в общем случае зависит от показателей элементов канала передачи информации: энергии сигнала, степени его ослабления в среде распространения, чувствительности и разрешающей способности приемника злоумышленника, уровня помех в канале и др. Чем длина канала больше, тем на большем удалении от источника возможно добывание информации и тем меньше риск злоумышленника. Если длина канала больше расстояния от источника сигнала до границы контролируемой зоны, то риск злоумышленника при добывании информации существенно меньше, так как он может разместить приемник сигнала за пределами контролируемой зоны. Поэтому злоумышленник стремится всеми возможными методами увеличить длину технического канала утечки информации.

Для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха. Это отношение достигается на различном удалении от источника сигнала, в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей — электромагнитная волна в длинноволновом диапазоне частот.

При определенной энергии сигнала требуемое отношение сигнал/шум обеспечивается (без учета спектральных характеристик

коэффициента затухания среды распространения) при более узкой полосе сигнала и канала. Поэтому, например, сужение полосы частот спектра сигнала радиозакладного устройства увеличивает дальность его приема. Наибольшую длину, за исключением случаев переноса материальных макротел как носителей информации, имеют радиоэлектронные каналы утечки информации. Длина составного канала утечки информации может быть сколь угодно большой.

Качественная оценка пропускной способности и длины технических каналов утечки информации указана в табл. 6.1.

*Таблица 6.1*

| № п/п | Вид канала | Показатели простого канала утечки информации | |
|---|---|---|---|
| | | Пропускная способность | Длина |
| 1 | Оптический | Высокая | В пределах прямой видимости |
| 2 | Акустический | Низкая | Малая (единицы — сотни м) |
| 3 | Радиоэлектронный | Высокая | Любая (сотни м — тысячи км) |
| 4 | Вещественный | Низкая | Любая |

Чем более широкую пропускную способность имеет канал утечки и чем он длиннее, тем большую потенциальную угрозу создает такой канал. Но рассмотренные показатели не учитывают ценность (полезность) предаваемой информации. При наличии канала утечки далеко не вся информация источника, имеющая определенную цену, попадет к злоумышленнику. Часть ее будет утеряна в канале утечки. Следовательно, цена информации, полученной злоумышленником, в общем случае всегда будет меньше цены информации источника. Поэтому важнейшим показателем технического канала утечки информации является его информативность. Однако информативность зависит, прежде всего, от информативности источника информации. Поэтому корректно говорить не об абсолютной информативности канала утечки, а об относительной информативности. Под **относительной информативностью технического канала** утечки понимается величина в интервале

0–1, соответствующая доли информации источника, которая может быть передана по рассматриваемому каналу. Например, оптический канал наблюдения за объектом разведки в помещении противоположного дома имеет высокую пропускную способность, но количество добываемой с его помощью информации зависит от разрешающей способности оптического приемника. Не вооруженный оптическим прибором наблюдатель может рассмотреть лишь крупные объекты, а с помощью специального телескопа можно прочесть текст документа в руках человека. Так как оптический приемник является элементом технического канала утечки информации, то его разрешающая способность характеризует относительную информативность этого канала.

Пропускная способность, длина и относительная информативность канала зависят от параметров его элементов: источника сигнала, среды распространения и приемника сигнала.

Источник сигнала характеризуется следующими показателями:

- мощностью сигнала;
- диаграммой направленности излучения сигнала (света, акустической и электромагнитной волн);
- параметрами спектра сигнала (шириной, неравномерностью спектральных составляющих);
- динамическим диапазоном сигнала.

Для технических каналов утечки информации характерна малая мощность носителя. Даже при перехвате сигналов функциональных служебных каналов связи прием сигналов, как правило, производится в стороне от направления «источник-приемник». Например, воздушная радиоэлектронная разведка во время барражирования самолета вдоль государственной границы способна перехватывать лишь боковые (существенно меньшие по мощности) излучения антенн передающих устройств достаточно близко расположенных у границы радиорелейных линий связи. Наименьшую мощность имеют сигналы побочных электромагнитных излучений и наводок радиоэлектронных и электрических приборов. Перехват таких сигналов стал возможен в середине XX в., что существенно повысило эффективность технической разведки.

**Диаграмма направленности излучения**, которая описывает характер распределения в пространстве энергии излучаемого (принимаемого) сигнала. Интегрально она оценивается шириной по уровню 0,5 мощности излучаемого поля в градусах в вертикальной и горизонтальной плоскостях — **шириной диаграммы направленности**. В отличие от антенн передатчиков и приемников функциональных радиоканалов связи, ширина которых устанавливается при создании антенн исходя из пространственного расположения источников и приемников сигналов, большинство антенн источников сигналов технических каналов утечки информации имеют так называемые **случайные антенны**. Функции случайных антенн могут выполнять любые проводники (ножки транзисторов, диодов и микросхем, провода, токопроводы печатных плат), по которым протекает электрический ток или в которых возникают высокочастотные электрические заряды. Так как эти токопроводящие элементы произвольно ориентированы по отношению к приемнику опасных сигналов, а их размеры не согласованы с длиной излучаемой волны, то более или менее достоверно можно описать диаграмму направленности случайной антенны только после проведения соответствующих инструментальных измерений. Мощность излучаемого случайной антенны электромагнитного поля зависит как от силы тока или величины заряда, так и от степени близости ее геометрических размеров длине волны. Чем они ближе, тем выше излучаемая мощность. Так как размеры случайных антенн малы (доли и единицы мм и см), то мощность излучения повышается при увеличении частоты колебаний зарядов или токов.

Основными показателями спектра сигнала, распространяющегося в техническом канале утечки информации, являются **ширина** и **неравномерность спектра** сигнала. Так как в отличие от функционального канала связи от канала утечки информации не требуется безыскаженная передача всех спектральных составляющих сигнала, а лишь тех, которые несут интересующую злоумышленника информацию, то важно при оценке канала утечки информации учитывать те области спектра, в которых сосредоточена основная энергия носителя. Такие области применительно к речевому сигналу называются фонемами. Например, в акустическом сигнале речевой информации при прохождении его через различные ог-

раждения помещения в большей степени поглощаются высокочастотные составляющие спектра речи, в результате чего на достаточно большом расстоянии исчезают признаки индивидуальности голоса говорящего человека, но смысл речевого сообщения остается понятным подслушивающему.

**Динамический диапазон сигнала оценивается** значением десятичного логарифма отношения максимальной мощности сигнала к минимальной. Значимость динамического диапазона для разных источников сигналов неодинаковая. Для оптического сигнала он имеет важное значение, так как описывает яркостные и цветовые отражательные свойства поверхности объекта. Для речевого сигнала его информативность существенно ниже, так как смысл речевого сообщения понимается даже при симметричном относительно нуля ограничении аналогового речевого сигнала и преобразовании его в двоичную последовательность — клипированную речь.

**Среда распространения** характеризуется набором физических параметров, определяющих условия распространения носителя с информацией. Основными из них являются:

- скорость распространения носителя в среде;
- коэффициент передачи или ослабления энергии носителя на единицу длины;
- зависимость коэффициента передачи от частоты сигнала (амплитудно-частотная характеристика);
- вид и мощность помех сигналу.

Если для носителя в виде радиоволны скорость распространения очень велика и ее можно не учитывать, то для носителей в виде материальных тел задержка носителя может привести к устареванию содержащейся на нем информации. Например, если достаточно долго не производился вывоз отходов делопроизводства из организации, то информация, содержащаяся в найденном на свалке черновике документа, может существенно потерять свою первоначальную цену.

При любом перемещении носителя в пространстве уменьшается его энергия. Мера снижения энергии зависит от вида носителя и характеристик среды. Например, бетонная стена не пропускает свет, существенно ослабляет акустическую волну и незначительно снижает энергию электромагнитной волны. Преодолевая различ-

ного рода препятствия на пути движения, злоумышленник устает, его движение замедляется и может вообще прекратиться. Так как любой физический сигнал — носитель информации может быть описан моделью в виде совокупности определенного набора колебаний (гармоник), а параметры среды относительно колебаний разных частот отличаются, то применительно к сигналам среда распространения может быть представлена в виде комплексного коэффициента передачи $K(\omega) = S(\omega)_{вых} / S_{вх}(\omega)$, где $S_{вх}(\omega)$ и $S_{вых}(\omega)$ — составляющие спектра (спектральные плотности) сигналов на входе и выходе среды распространения соответственно. Коэффициент передачи $K(\omega)$ представляет собой **амплитудно-частотную характеристику (АЧХ)** среды распространения технического канала утечки информации.

Среда распространения, как правило, неоднородная. Ее АЧХ зависит от параметров рассматриваемой среды распространения, которые могут изменяться в зависимости от большого числа природных и искусственных факторов. Например, на условия распространения радиоволн влияет концентрация ионов в атмосфере, которая зависит от солнечной радиации, изменяющейся в дневное и ночное время суток. Любую среду можно представить в виде последовательно соединенных n участков с одинаковыми характеристиками каждого из участков АЧХ: воздух-стекло-воздух-стекло, воздух-бетонная стена-воздух-кирпичная стена-воздух и др. Если коэффициент передачи i-го элемента среды распространения $K_i(\omega)$, то коэффициент передачи среды $K_{ср}(\omega) = \prod_{i=1}^{n} K(\omega)$. Следовательно, коэффициент затухания среды определяется, прежде всего, ее участком с наибольшим затуханием. Результаты качественного анализа разных сред распространения приведены в табл. 6.2.

*Таблица 6.2*

| *№ п/п* | *Вид носителя* | *Вид среды распространения* | *Затухание среды* | *Длина канала* |
|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* |
| 1 | Видимый и ИК свет | Безвоздушное пространство | Очень малое | В пределах прямой видимости |
| | | Атмосфера | Малое | |
| | | Оптическое волокно | Очень малое | |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 2 | Радиосигнал | Безвоздушное пространство<br>Атмосфера<br>Твердые тела | Очень малое<br><br>Очень малое<br>Для диэлектриков — малое | От прямой видимости до очень большой |
| 3 | Электрический сигнал | Электрический провод | Определяется электрическим сопротивлением материала | Без ретрансляции сотни-тысячи м |
| 4 | Акустический сигнал | Атмосфера<br>Вода<br>Твердое тело | Большое<br>Малое<br>Очень малое | Очень малая<br>Малая<br>Малая |
| 5 | Материальное тело | Макротела | | Произвольная |

От параметров **приемника сигналов** существенно зависят характеристики технического канала утечки информации. Основными параметрами приемника сигналов являются:

- диапазон принимаемых частот;
- чувствительность;
- пространственная селективность приемной антенны;
- динамический диапазон сигнала;
- вид и уровень искажений сигнала.

Очевидно, что диапазон частот (длин волн) приемника должен соответствовать диапазону частот (длин волн) сигнала. Но так как частоты источника сигнала случайного канала не известны злоумышленнику, то для поиска и приема используется приемник с диапазоном частот, охватывающим возможные частоты сигнала. Например, современные сканирующие радиоприемники имеют перестраиваемый диапазон частот от долей до нескольких десятков тысяч МГц.

Различают предельную и реальную чувствительность приемника. Так как в любом приемнике сигналов производится преобразование сигнала любого вида в электрический сигнал, то **предельная чувствительность** определяется уровнем собственных тепловых шумов входных электрических цепей приемника. Эти шумы ограничивают возможности любого приемника. **Реальная чувст-**

**вительность** учитывает качество информации на выходе приемника и характеризуется минимальным уровнем сигнала на входе, при котором отношение сигнал/шум на его выходе соответствует заданному значению. Ухудшают качество информации на выходе приемника не только собственные шумы, но и уровень помех в среде распространения, который может быть выше уровня собственных шумов.

**Динамический диапазон** приемника характеризуется отношением в логарифмическом масштабе максимального и минимального уровней входного сигнала, при котором обеспечивается требуемый уровень качества сигнала на выходе приемника. При малом динамическом происходит искажение сигнала большой амплитуды. Так как приемники технических каналов утечки информации имеют высокую чувствительность, то из-за непостоянства коэффициента затухания среды во времени возможен уровень входного сигнала, который при определенном коэффициенте усиления вызывает ограничение выходного сигнала, что приводит к заметным его искажениям. Например, закладное устройство, рассчитанное на уровень акустического сигнала, соответствующего нескольким метрам от источника звука, при приближении этого источника к месту нахождения закладного устройства будет излучать радиосигнал с искаженной речевой информацией. С целью расширения динамического диапазона приемника в нем предусматривают автоматическую регулировку усиления (АРУ) в зависимости от среднего уровня входного сигнала.

Несоответствие спектральных характеристик и динамического диапазона приемника соответствующим характеристикам входного сигнала, воздействие внешних помех и тепловых шумов, неэквивалентное усиление наведенного в антенне приемника для разных частотах и разных уровней приводят к частотным и нелинейным искажениям сигнала на входе демодулятора. Так как искажение параметров сигнала вызывает изменение информации, то сигналы на выходе демодулятора содержат уже измененную информацию.

Для составных каналов утечки информации значения всех рассмотренных показателей, за исключением мощности сигнала на входе приемника, ухудшаются, так как при любом преобразова-

нии сигнала происходит изменение его информативных параметров, следовательно, и информации. А так как качество любого канала связи оценивается по подобию полученной информации переданной, то любое уменьшение подобия может трактоваться как ухудшение качества информации. Конечно, в большинстве случаев к качеству информации на выходе технического канала утечки предъявляются менее жесткие требования, чем к функциональному каналу связи. Но далеко не всегда. При передаче цифровых данных трансформация чисел может доставить злоумышленнику столь же большие неприятности, как и санкционированному получателю.

## 6.4. Комплексное использование технических каналов утечки информации

Многообразие каналов утечки информации предоставляет злоумышленнику большой выбор путей, способов и средств добывания информации. На основе результатов анализа каждого из рассмотренных каналов можно сделать следующие выводы.

1. Утечка семантической информации возможна по всем техническим каналам. По совокупности угроз информации каналы ее утечки можно проранжировать в следующей последовательности: радиоэлектронный, акустический и оптический каналы. Однако в некоторых конкретных условиях возможны иные ранги каналов, например когда имеется реальная предпосылка для наблюдения или фотографирования документов.

2. Наибольшими потенциальными возможностями по добыванию информации о видовых демаскирующих признаках обладает оптический канал, в котором информация добывается путем фотографирования. Это обусловлено тем, что фотоизображение имеет:

- самое высокое разрешение даже на большом расстоянии от объекта наблюдения, например, при детальной фотосъемке из космоса оно достигает 10–15 см на местности;
- самую высокую информационную емкость, обусловленную максимумом демаскирующих признаков, в том числе наличием такого информативного признака как цвет.

Информационные объемы телевизионных изображений примерно на порядок ниже фотоизображений. Телевизионные изоб-

ражения имеют худшее разрешение, повышенный уровень яркостных искажений за счет неравномерности спектрально-яркостных характеристик фотокатода передающих телевизионных трубок или приборов с зарядовой связью, повышенный уровень геометрических искажений за счет дополнительных искажений при формировании электронного растра.

Изображения в ИК-диапазоне обладают еще более низкими информационными параметрами. Кроме низкой разрешающей способности и больших искажений для изображений в ИК-диапазоне характерна крайняя изменчивость яркости в течение суток. Однако, как уже отмечалось при рассмотрении каналов утечки информации, изображение в каждом из них содержит дополнительные признаки за счет различной их природы.

3. Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный. В значительно меньшем объеме утечка информации о сигнальных демаскирующих признаках возможна в акустическом и вещественном каналах.

Различия в характеристиках технических каналов утечки информации и распространяемой по ним информации используются разведкой для повышения эффективности добывания информации путем их комплексного использования. Комплексное использование заключается в добывании информации по одному тематическому вопросу по нескольким параллельным или последовательным каналам утечки.

Комплексное использование параллельных каналов утечки информации основывается на следующих принципах:

- комплексируемые каналы дополняют друг друга по своим возможностям;
- эффективность комплексирования повышается при уменьшении зависимости между источниками информации и демаскирующими признаками в разных каналах.

Комплексирование каналов утечки информации обеспечивает:

- увеличение вероятности обнаружения и распознавания объектов за счет расширения их текущих признаковых структур;
- повышение достоверности семантической информации и точности измерения признаков, в особенности в случае добывания информации из недостаточно надежных источников.

Когда возникают сомнения в достоверности информации, то с целью исключения дезинформации полученные сведения и данные перепроверяют по другому каналу.

Возможны два основных вида комплексирования каналов утечки информации — обеспечение утечки информации от одного источника по нескольким параллельно функционирующим каналам связи (см. рис. 6.4а)) и от разных источников (рис. 6.4б)).

В первом варианте одна и та же информация распространяется по различным направлениям одним или разными носителями. Например, речевая информация разговаривающих в помещении людей может быть подслушана через дверь или стену, снята с опасных сигналов или передана с помощью закладного устройства.

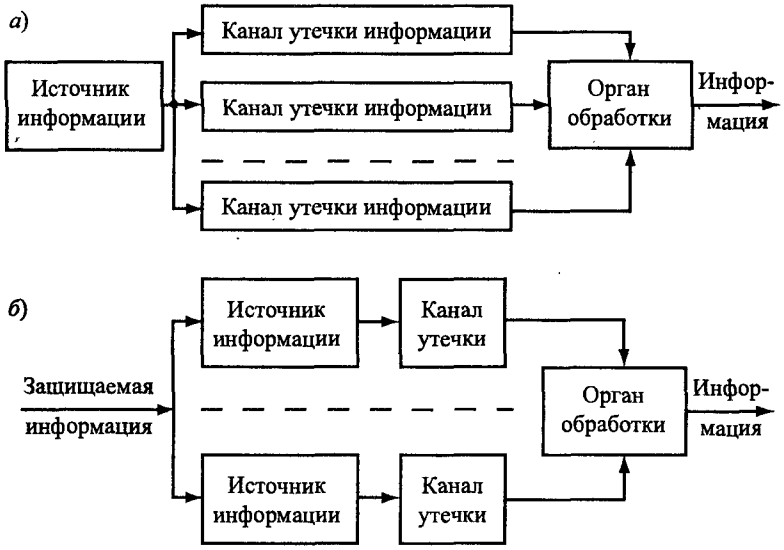



*Рис. 6.4.* Варианты комплексного использования каналов утечки информации

Так как вероятность воздействия помех в разных каналах на одинаковые элементы информации мала, то в этом случае повышается достоверность суммарной информации после обработки ее в соответствующем органе. При независимости помех в n-каналах утечки информации вероятность поражения одного и того же элемента информации при комплексировании n каналов рассчитывается по формуле:

$$P_n = \prod_{i=1}^{n} P_i,$$

где $P_i$ — вероятность поражения элемента информации в i-м канале.

Однако если источник не владеет достоверной информацией или занимается дезинформацией, то рассмотренный вариант комплексирования не повышает достоверность итоговой информации. Для обеспечения такой возможности одна и та же информация добывается от нескольких источников, например из документа и от специалистов, участвующих в создании этой информации (рис. 6.4б)). При таком комплексном использовании 2 каналов вероятность внедрения дезинформации можно оценить по формуле:

$$P_д = P_1 P_2 + r\sqrt{P_1(1-P_1)P_2(1-P_2)},$$

где $P_1$ и $P_2$ — значения вероятности появления дезинформации в 1-м и 2-м каналах; r — коэффициент корреляции между информацией в этих каналах.

Коэффициент r корреляции характеризует статистическую зависимость между информацией в разных каналах. При r = 1 по каналам производится утечка информации одинакового содержания или об одинаковых признаках, при r = 0 — источники независимые. Как следует из этой формулы, для уменьшения риска получения дезинформации необходимо снижать коэффициент корреляции между источниками информации.

Последовательное соединение каналов, как следует из их анализа в предыдущих подразделах, обеспечивает, прежде всего, увеличение длины канала, что снижает риск органа разведки (злоумышленника). Фактически каждый последующий канал обеспечивает ретрансляцию сигналов предыдущего канала. Так как акустический канал имеет наименьшую длину, то часто с ним последовательно соединяются другие каналы: радиоэлектронные и оптические. Если возникает необходимость наблюдения в закрытом от постороннего взора помещении, то это становится возможным при ретрансляции оптического сигнала, формирующего изображение, по радиоэлектронному каналу, сигналы которого проникают через стены или зашторенные окна помещения.

## 6.5. Акустические каналы утечки информации

В акустическом канале утечки носителем информации от источника к несанкционированному получателю является акустическая волна в атмосфере, воде и твердой среде. Структура канала утечки информации приведена на рис. 6.5.

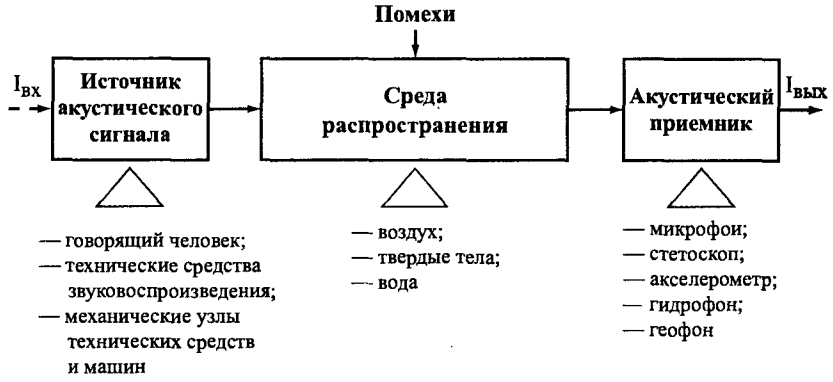



*Рис. 6.5.* Структура акустического канала утечки информации

Источниками акустического сигнала могут быть:

- говорящий человек или озвучивающее его речь звуковоспроизводящее устройство;
- механические узлы механизмов и машин, которые при работе создают акустические волны.

Акустические речевые сигналы создает **речевой аппарат человека**, голосовой тракт которого представляет собой трубку со средней длиной у взрослого мужчины примерно 17 см и с переменной площадью поперечного сечения. Вход в голосовой тракт образуют голосовые связки, а выход — губы. Поперечное сечение может изменяться при движении артикулярных органов — губ, челюстей, языка и небной занавески (мягкого неба), являющейся продолжением твердого неба, от полного закрытия до величины более 20 см$^2$.

Вспомогательный путь распространения звуковых колебаний образует носовой тракт, который начинается у небной занавески и заканчивается ноздрями. Опусканием или поднятием небной занавески регулируется связь между носовой и ротовой полостями,

которая существенным образом влияет на характер произносимых звуков.

Источником энергии при речеобразовании служит поток воздуха, выталкиваемого из легких при сжимании грудной клетки ее мускулатурой. Воздух проходит по трахее в полость глотки. Сверху трахея заканчивается гортанью. На хрящевой основе гортани укреплены 2 пленки из связочной и мышечной ткани, которая называется **голосовыми связками**. Щелевой проход между связками образует **голосовую щель**. При прохождении под давлением воздуха через голосовую щель связки колеблются с частотой, определяемой в основном массой и упругостью связок и величиной подсвязочного давления воздуха. Основная частота колебаний голосовых связок называется частотой **основного тона**. Частота (высота) основного тона характеризует собой тип голоса говорящего: бас, баритон, тенор, альт, контральто, сопрано. Частоты основного тона указанных типов голосов находятся в интервале 80–300 Гц, но различия частот слабо влияют на показатели распознавания звуков речи.

Сила воздушного потока, прошедшего через голосовую щель и определяющая громкость речевого сигнала, зависит от площади щели и подсвязочного давления воздуха. Для очень громких звуков в легких создается давление порядка 20 см водяного столба.

Толчки или импульсы воздуха, прошедшего через колеблющиеся голосовые связки, возбуждают акустическую систему над голосовыми связками. Форма импульсов, образуемых голосовой щелью, в процессе разговора, сильно изменяется в зависимости от частоты основного тона и интенсивности звука. Звуки малой интенсивности и с низкой частотой основного тона имеют низкое подсвязочное давление, большую скважность и небольшую амплитуду импульсов. При средних громкости и частоте основного тона импульсы имеют треугольную форму, частотный спектр которой богат гармониками или обертонами. Длительность импульсов составляет всличину порядка 0,3–0,7 периода колебаний. Звуки большой интенсивности и с высокой частотой основного тона характеризуются высоким подсвязочным давлением, небольшой скважностью и большой амплитудой.

Кроме того, голосовой тракт возбуждает турбулентный поток воздуха в точках сужения и изменения давления воздуха, создаваемого в области смычки губ, зубов или неба. При раскрытии смычки речевой тракт возбуждается в результате возникающего в нем переходного процесса.

При возбуждении голосового тракта колебаниями голосовых связок образуются гласные звуки, звонкие (вокализованные) согласные звуки — совместно голосовым и шумовым источниками, а глухие — только шумовыми источниками.

Спектр речевого сигнала после прохождения резонаторов голосового тракта, образуемых воздушными объемами полости рта и носоглотки, изменяется в процессе произнесения различных звуков и зависит от положения языка и зубов. При этом одни гармонические составляющие усиливаются, другие подавляются. Области спектра звука, в которых сосредоточивается основная мощность акустического сигнала, называются **формантными областями** или **формантами**. Большинство звуков речи имеют одну или две форманты, что обусловлено участием в образовании звуков резонаторов голосового тракта полостей рта и носоглотки. Форманты звуков речи расположены в области частот от 150–200 Гц до 8600 Гц. Например, гласный звук «а» имеет одну форманту полосой 1100–1400 Гц, звук «э» — две форманты в полосах 600–1000 Гц и 1600–2500 Гц, согласный звук «л» — две форманты (200–500 Гц), звук «ш» — одну форманту полосой 1200–6300 Гц. Но основная энергия подавляющей части формант сосредоточена в диапазоне частот 300–3000 Гц, что позволило ограничить спектр речевого сигнала, передаваемого по стандартному телефонному каналу, этой полосой. Гласные звуки имеют выраженный дискретный спектр, согласные звуки характеризуются либо сплошным спектром, либо наличием сплошного спектра в отдельных полосах частот.

Средняя длительность различных звуков речи существенно различается в диапазоне 20–260 мс. Гласные звуки более длительные, чем согласные, наибольшая длительность отмечается для звука «а», наименьшая — для звука «п». Длительность ударных гласных звуков больше, чем неударных.

Психологическая (с учетом чувствительности уха на разных частотах) интенсивность акустических сигналов изменяется в ши-

роких пределах 0–130 дБ. Для человека как основного источника соотношение между уровнем громкости и его качественной оценкой характеризуется следующими данными: очень тихая речь (шепот) — 5–10 дБ, тихая речь — 30–40 дБ, речь умеренной громкости — 50–60 дБ, громкая речь — 60–70 дБ, крик — 70–80 дБ и более. Громкость крика школьников одной из лондонских школ во время соревнования по крику составляла в среднем 114 дБ, а победительницы — 122 дБ. Сила голоса певцов достигает 130 дБ на расстоянии 1 м от певца. Во времена, когда певцы не пользовались микрофонами для усиления громкости звука, первоклассный вокалист должен был мощью своего голоса покрывать, например, пространство, на котором могут разместиться до 300 слушателей. Для сравнения: фортиссимо большого симфонического оркестра составляет 90 дБ, вой сирены «скорой помощи» — 100 дБ, а шум реактивного двигателя на расстоянии 5 м — 120 дБ.

Уровень речи во время речеобразования непрерывно меняется. Поэтому интенсивность речи характеризуют **средним уровнем интенсивности речи** и **средним спектральным уровнем речи** — средним уровнем энергии, приходящейся на полосу шириной 1 Гц. Разность между пиковым (максимальным) значением речевого сигнала и его средним уровнем называют **пикфактором речи**.

Так как основным приемником звуковых волн является слуховая система человека, субъективное восприятие которым интенсивности речи зависит не только от величины звукового давления звуковой волны на мембрану уха, но и от ее частоты, то для оценки энергетического показателя звука, учитывающего возможности слуха человека, введено понятие **громкости звука**. Громкость звука представляет собой взвешенную по частоте интенсивность звука.

Кроме громкости речь человека характеризуется тоновым диапазоном (диапазоном частот), тембром и вибрато.

Среднестатистический голос человека включает тоны (частоты) в диапазоне 64–1300 Гц. Крайне низкие тоны басовых голосов имеют частоту около 40 Гц, высокие тоны детских голосов — около 4000 Гц. При разговоре изменение тона составляет обычно 0,1 диапазона голоса, изменение тона певческого мужского голоса достигает около 2,5 октавы, женского — 3 октавы.

Тембр голоса человека определяется количеством и величиной гармоник (обертонов) его спектра. Обертоны создаются голосовыми связками и усиливаются резонаторами гортани, рта и различных полостей-пазух головы человека (верхней челюсти, лобной, основной, решетчатой, полости носа). Резонаторы человека относятся к трубчатым воронкообразным и полостным резонаторам. Трубчатые резонаторы содержат медные духовые инструменты, полостные — корпуса струнных инструментов (гитары, скрипки и др).

Вибрато представляет собой периодическое изменение высоты и силы голоса с частотой примерно 5–7 пульсаций в секунду. При отсутствии вибрато голос кажется безжизненным и невыразительным.

Значения характеристик голоса конкретного человека индивидуальные и позволяют идентифицировать человека по его голосу.

Акустические сигналы машин и технических средств возникают в результате колебаний их поверхностей и частиц воздуха, проходящего через различные отверстия и полости машин и средств.

В общем случае диапазон частот акустических сигналов составляет:

- менее 16 Гц (в инфразвуковом диапазоне) — вибрации машин;
- 16 Гц–20 кГц (звуковой диапазон) — речь, звуки машин;
- более 20 кГц (ультразвуковой диапазон) — звуки отдельных живых существ и механических средств.

Источники сигналов характеризуются **диапазоном частот**, **мощностью излучения** в Вт, **интенсивностью излучения** в Вт/м$^2$ — **мощностью акустической волны**, прошедшей через перпендикулярную поверхность площадью 1 м$^2$, **громкостью звука** в дБ, измеряемой как десятичный логарифм отношения интенсивности звука к порогу слышимости. Интенсивность излучения является физической характеристикой акустического сигнала, а громкость — физиологической, учитывающей разную чувствительность слуховой системы человека к акустическим волнам разной частоты. Уровни громкости различных источников иллюстрируются данными табл. 6.3.

*Таблица 6.3*

| *Оценка громкости звука на слух* | *Уровень звука, дБ* | *Источник звука* |
|---|---|---|
| Очень тихий | 0 | Усредненный порог чувствительности уха |
| | 10 | Тихий шепот (1,5 м) |
| Тихий | 20 | Тиканье настенных механических часов |
| | 30 | Шаги по мягкому ковру (3–4 м) |
| | 40 | Тихий разговор, шум в читальном зале |
| Умеренный | 50 | Шум в жилом помещении, легковой автомобиль (10–15 м) |
| | 60 | Улица средней шумности |
| Громкий | 70 | Громкая речь (1 м), зал большого магазина |
| | 80 | Радиоприемник громко (2 м), крик |
| Очень громкий | 90 | Шумная улица, гудок автомобиля |
| | 100 | Симфонический оркестр, автомобильная сирена |
| Оглушительный | 110 | Пневмомолот, очень шумный цех |
| | 120 | Гром над головой |
| | 130 | Звук воспринимается как боль |

Так как основным источником акустической речевой информации является человек, то средняя мощность (громкость) источников сигналов акустических каналов утечки информации составляет 40–80 дБ.

Следует отметить, что, хотя громкость звуков в логарифмическом масштабе принимает значения десятков дБ, абсолютная величина их мощности крайне мала. Например, акустической энергии непрерывного громкого разговора жителей Москвы в течение суток хватит лишь на то, чтобы вскипятить чайник с водой.

Физические явления, возникающие при распространении акустических волн, изучаются физической акустикой. В воздушной среде акустический сигнал распространяется в виде продольной упругой волны, которая представляет собой колебание частиц воздуха вдоль направления распространения волны. Продольные колебания воздуха приводят к изменению давления относительно ат-

мосферного в области распространения волны. Звуковое давление, соответствующее порогу слышимости уха, составляет $10^{-10}$ от нормального атмосферного, болевому порогу — порядка $10^{-4}$ от атмосферного давления.

В твердых телах наряду с продольными волнами возникают поперечные (перпендикулярные направлению распространения волны) колебания, которые не создают давления в продольном направлении.

Акустические волны как носители информации характеризуются следующими показателями и свойствами:

- энергией (мощностью);
- скоростью распространения носителя в определенной среде;
- величиной (коэффициентом) затухания или поглощения;
- условиями распространения акустической волны (коэффициентом отражения от границ различных сред, дифракцией).

Теоретически скорость звука определяется формулой Лапласа:

$$C_{зв}=\sqrt{K/\rho}\,,$$

где K — модуль всесторонней упругости (когда сжатие производится без притока и отдачи тепла) вещества среды распространения; ρ — плотность вещества среды распространения.

Для газов модуль всесторонней упругости равен их давлению. При сжатии газа увеличение давления сопровождается пропорциональным увеличением его плотности. Поэтому скорость звука в газе не зависит от его плотности, а пропорциональна корню квадратному из температуры газа, значению универсальной газовой постоянной, отношению величин теплоемкостей газа при постоянном объеме и давлении.

Скорость звука в морской воде зависит от ее температуры, солености и давления на рассматриваемой глубине, а в твердых телах определяется, в основном, плотностью и упругостью веществ.

Значения скорости распространения звука в некоторых типичных средах приведены в табл. 6.4.

*Таблица 6.4*

| *Среда распространения* | *Скорость, м/с* |
|---|---|
| Воздух при температуре:<br>0° С<br>+20° С | <br>332<br>344 |
| Вода морская | 1440–1540 |
| Железо | 4800–5160 |
| Стекло | 3500–5300 |
| Дерево | 4000–5000 |

*Примечание.* Разброс значений скорости обусловлен отличиями свойств среды распространения.

**Среда распространения носителя информации** от источника к приемнику может быть однородной (воздух, вода, твердые тела) и неоднородной, образованной последовательными участками различных физических сред: воздуха, древесины дверей, стекол окон, бетона или кирпича стен, различными породами земной поверхности и т. д. Но и в однородной среде ее параметры не постоянные, а могут существенно различаться в разных точках пространства.

При распространении звуковых колебаний движение частиц среды вызывает давление во фронте волны. **Фронтом звуковой волны** называется поверхность, соединяющая точки поля с одинаковой фазой колебания. По мере распространения в любой среде звуковые волны затухают.

Затухание акустической волны в воздухе вызвано:

- расхождением акустической волны в пространстве;
- рассеянием акустической волны на неоднородностях воздушной среды (каплях дождя, снежинках, пыли, ветках деревьев и др.);
- турбулентностью воздушных потоков, вызванной неравномерным распределением в пространстве температуры, давления, силы и скорости ветра, которые искривляют акустическую волну и вызывают частичное ее отражение от границы раздела слоев воздуха с различными плотностями.

Интенсивность сферической акустической волны (в виде сферы) в результате расхождения убывает обратно пропорционально

расстоянию от источника, а амплитуда звукового давления — обратно пропорционально расстоянию. Если среда ограничена отражающей поверхностью, то степень затухания уменьшается. В металлических звуководах и в трубах большая часть энергии звуковой волны многократно переотражается от стен и в пространстве рассеивается в существенно меньшей степени. Поэтому дальность распространения акустической волны в них значительно больше.

Дальность подслушивания повышается утром и вечером, в пасмурную погоду и после дождя, над водной поверхностью, зимой при отсутствии снегопада, в горах за счет переотражений от них, а также если ветер дует со стороны источника звука. Дождь, снег, встречный (по направлению к источнику звука) ветер могут увеличить затухание акустической волны на 8–10 дБ для расстояния 100 м. При звуке, направленном против ветра, лучи акустической волны изгибаются вверх и могут пройти выше стоящего на земле человека, а при звуке по ветру они изгибаются вниз, увеличивая дальность слышимости с подветренной стороны. Затухание звуковых волн в морской воде больше, чем в дистиллированной, и меньше (почти в 1000 раз), чем в воздухе.

Так как акустическая волна распространяется в результате передачи энергии колебаний от одной микрочастицы среды к другой, то чем выше частота колебаний, тем большая энергия нужна для раскачивания соседней микрочастицы. Поэтому затухание звука в среде распространения пропорционально квадрату частоты колебаний.

При распространении акустической волны в среде ее траектория изменяется в результате отражений и дифракции. На границе сред с разной плотностью акустическая волна частично переходит из одной среды в другую, частично отражается от границы между двумя средами. При падении звука из воздуха на воду, бетон, дерево в эти среды проникает не более сотых долей мощности звука.

Отражение звука происходит также от поверхностей разделов слоев воздуха (воды) с разными значениями акустического сопротивления вследствие неодинаковой температуры и плотности. Этим объясняются значительные колебания (в 10 и более раз) дальности распространения звука в атмосфере.

При определенных условиях неоднородности создают условия для образования **акустических (звуковых) каналов**, по которым акустическая волна может распространяться на значительно большие расстояния, как свет по оптическим световодам. Акустические каналы чаще всего образуются в воде морей и океанов на определенной глубине, на которой в результате влияния двух противоположных природных факторов (плотности воды и ее температуры) создается акустический канал с меньшей скоростью распространения, чем в выше- и нижерасположенных слоях воды. Такое явление возникает потому, что скорость распространения акустической волны в воде увеличивается с глубиной из-за повышения плотности воды и уменьшается при понижении ее температуры в более глубоких слоях, особенно в летнее время. В слоях ниже акустического канала преобладает влияние первого фактора, способствующего увеличению скорости акустической волны, выше — второго фактора. Акустическая волна, попадающая в эту область, распространяется внутри ее с соответствующим для параметров воды затуханием. При отклонении траектории распространения волна, преломляясь в неоднородностях области, возвращается в канал. В результате этого длина акустического канала существенно увеличивается. Звуковая волна от подводных взрывов может распространяться на расстояние в сотни км.

В помещении акустическая волна многократно отражается от ограждений, в результате чего в нем возникает сложное акустическое поле в виде совокупности волн, приходящихся непосредственно от источника и отраженных. Акустические сигналы при прохождении через вентиляционные воздухопроводы ослабевают из-за поглощения в стенах короба и в изгибах. Однако за счет многократных переотражений акустической волны от стенок воздуховода ее энергия не рассеивается в пространстве. Вследствие этого дальность распространения волны в воздуховоде может быть существенно больше, чем в свободном пространстве. Затухание в прямых металлических воздуховодах составляет 0,15 дБ/м, в неметаллических — 0,2–0,3 дБ/м. При изгибах затухание достигает 3–7 дБ (на один изгиб), при изменениях сечения — 1–3 дБ. Ослабление сигнала на выходе из воздуховода помещения составляет 10–16 дБ [14].

За счет многократных переотражений акустической волны в замкнутом пространстве возникает явление послезвучания — **реверберация**. Величина реверберации оценивается временем реверберации $T_р$, равного времени уменьшения интенсивности звука после выключения его источника на 60 дБ. Вследствие многократных переотражений в помещении на барабанную перепонку человека или мембрану микрофона оказывают давление акустические волны, распространяющиеся разными путями от источника звука. При очень малом значении времени реверберации на барабанную перепонку или микрофон воздействует, в основном, быстро затухающая прямая волна. В этом случае слышимость речи при удалении от источника резко уменьшается, а тембр звуков речи за счет большего затухания в воздухе высоких частот обедняется, что ухудшает слышимость речи в крупных помещениях. Чем больше размеры помещения и меньше коэффициент поглощения ограждающих поверхностей, тем больше время реверберации. При большем времени реверберации слышимость в удаленных от источника звука точках пространства улучшается за счет энергии отраженных от стен акустических волн. Но при большом времени реверберации на звуки, создаваемые в текущий момент времени, накладываются предшествующие звуки, что ухудшает разборчивость речи и делает помещение гулким. Поэтому для каждого помещения существует оптимальное время реверберации, при котором обеспечиваются хорошие слышимость и разборчивость речи или музыки. Время реверберации менее 0,85 с незаметно для слуха. Для большинства типовых помещений организаций время реверберации мало (0,2–0,6 с) и его можно не учитывать при оценке разборчивости.

Для концертных залов, имеющих существенно большие размеры, время реверберации определяет их акустику. Установлено, что в помещениях объемом до 350 м$^2$ оптимальной является реверберация со временем до 1,06 с. При увеличении объема помещения $V_п$ время реверберации пропорционально повышается и принимает для $V_п = 27000$ м$^3$ значение около 2 с.

Время реверберации в помещении объемом $V_п$ может быть вычислено по приближенной формуле Сэбина:

$$T_р = 0{,}16V_л / S\alpha_{сп},$$

где S — суммарная площадь поверхности помещения в м$^2$; $\alpha_{сп} = \sum_{\forall k} \alpha_k S_k$ — средний коэффициент звукопоглощения в помещении; $S_k$ и $\alpha_k$ — площадь и коэффициент поглощения k-й ограждающей поверхности соответственно.

При распространении структурного звука в конструкциях зданий, особенно в трубопроводах, также возникают реверберационные явления, искажающие акустический сигнал и снижающие разборчивость речи на 15–20%. Следовательно, в замкнутом помещении акустическое поле представляет собой сумму «прямого» звука и отраженных акустических волн, образующих диффузное поле. Характер диффузного поля влияет на качество принимаемого звука. Это влияние оценивают коэффициентом — акустическим отношением, равным отношению суммарного уровня отраженных волн к уровню прямой волны. Акустическое отношение может достигать величины 10–15. Однако при значении акустического отношения более 4 ухудшается четкость звучания — возникает гулкость звука. Четкость звучания оценивается отношением плотности энергии звука, приходящего в точку измерения (приема) в течение 60 мс и воспринимаемого слушателем слитно, к общей плотности энергии звука в этой точке. Чем больше четкость звучания, тем меньше влияние запаздывающих отраженных акустических лучей.

Качество слышимой речи субъективно оценивается градациями ее **понятности**: отличная, хорошая, удовлетворительная, предельно допустимая. Слышимая речь характеризуется как отличная, если все слова, даже незнакомые, например фамилии, воспринимаются во время разговора без переспроса. Если во время разговора переспрашиваются отдельные незнакомые слова, то речь оценивается как хорошая. Частые переспросы характеризуют речь как удовлетворительную. Если возникает потребность в переспросе слов по отдельным буквам, то речь является предельно допустимой. Оценки понятности речи на основе данных [15] в некоторых возможных местах нахождения средств подслушивания приведены в табл. 6.5.

*Таблица 6.5*

| *№ п/п* | *Место нахождения злоумышленника или его технического средства* | *Понятность речи* |
|---|---|---|
| 1 | За окном на расстоянии 1–1,5 м от оконной рамы при закрытой форточке | Предельно допустимая |
| 2 | За окном на расстоянии 1–1,5 м при открытой форточке | Хорошая |
| 3 | На оконной раме или внешнем оконном стекле при закрытой форточке | Предельно допустимая |
| 4 | За дверью (без тамбура) | Хорошая |
| 5 | За перегородкой из материала типа гипсолит или асбетоцемент | Предельно допустимая |
| 6 | На перегородке из материала типа гипсолит или асбетоцемент | Удовлетворительная |
| 7 | На железобетонной стене | Удовлетворительная — хорошая |
| 8 | В воздуховоде (6–8 м от ввода) | Удовлетворительная |
| 9 | На трубопроводе (через этаж) | Хорошая |

Как следует из данных таблицы, понятность речи за пределами помещения может быть достаточной для образования каналов утечки информации.

Понятность речи зависит также от уровня и характера помех в среде распространения. Акустические помехи (шумы) вызываются многочисленными источниками — автомобильным транспортом, ветром, техническими средствами в помещениях, разговорами в помещениях и т. п. Уровни шумов изменяются в течение суток, дней недели, зависят от погодных условий. Ночью и в выходные дни шумы меньше. Усредненные значения акустических шумов в помещении и вне его на частоте 1000 Гц приведены в табл. 6.6 [16].

*Таблица 6.6*

| *Акустические шумы в помещениях* | *Уровень шума в дБ* | *Акустические шумы вне зданий* | *Уровень шума в дБ* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| Комната тихая | 25–30 | Тихая улица (без движения автотранспорта) | 30–35 |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Комната шумная | 40–50 | Средний шум на улице | 55–60 |
| Кабинет при одном работающем | 20–25 | Шумная улица без трамвайного движения | 60–75 |
| Спокойный разговор 3 человек | 45–50 | Легковой автомобиль в городе на расстоянии 10–20 м | 50–65 |
| Громкий разговор по телефону | 55 | Грузовой автомобиль в городе на расстоянии 10–20 м | 60–75 |
| Обычный разговор на расстоянии 1 м | 55–60 | Троллейбус на расстоянии 5 м | 75 |
| Громкий разговор на расстоянии 1 м | 65–70 | Трамвай на расстоянии 10–20 м | 80–85 |
| Шумное собрание | 65–70 | Электропоезд на эстакаде на расстоянии 6 м | 90 |
| Коридор | 35–40 | | |

Санитарные нормы уровня шумов на частоте 1000 Гц, допустимые для сна и отдыха, составляют 35 дБ, для умственной работы — 45 дБ, для обеспечения речевой и телефонной связи — 50 дБ, для труда в офисе — 55 дБ.

**Акустические приемники** обеспечивают селективность акустических сигналов в пространстве и по частоте, преобразование их в электрические сигналы, усиление электрических сигналов, консервацию и преобразование их в форму, доступную для восприятия информации человеком. В зависимости от среды распространения акустической волны различают акустоэлектрические преобразователи акустических приемников: в атмосфере — микрофоны, в твердой среде — стетоскоп и акселерометр, в воде — гидрофон и земной поверхности — геофон. Ухо имеет наибольшую чувствительность в средней области звукового диапазона (1500–2000 Гц) и меньшую чувствительность на низких и высоких частотах. Средний порог слышимости человека соответствует мощности звука $10^{-12}$ Вт или звуковому давлению на барабанную перепонку уха человека $2 \cdot 10^{-5}$ Па. В диапазоне 250–500 Гц происходит ухудшение слышимости и, следовательно, громкости примерно на 6 дБ. Акустические шумы при восприятии речи человеком повышают порог его слышимости.

Дальность акустического канала утечки информации, в осо бенности от такого источника как человек, мала и, как правило, н обеспечивает возможность ее съема за пределами территории орга низации. Речь человека при обычной громкости может быть непос редственно подслушана злоумышленником на удалении единиц к в редких случаях — десятков метров.

Поиски путей повышения дальности добывания речевой ин формации привели к появлению составных каналов утечки инфор мации. Применяются два вида составного канала утечки информа ции: акусто-радиоэлектронной и акусто-оптический.

**Акусто-радиоэлектронный канал утечки информации** со стоит из двух последовательно сопряженных каналов: акустическо го и радиоэлектронного каналов утечки информации. Приемником акустического канала является функциональный или случайно об разованный акустоэлектрический преобразователь. Электрический сигнал с его выхода поступает на вход радиоэлектронного канал утечки информации — источника электрических или радиосигна лов.

Структура акусто-радиоэлектронного канала утечки информа ции приведена на рис. 6.6.


*Рис. 6.6.* Структура акусто-радиоэлектронного канала утечки информации

Акустоэлектрический преобразователь образует источник опасных сигналов и реализуется в закладном устройстве, разме щаемом злоумышленником в помещении. Закладные устройства создаются специально для подслушивания речевой информации и обеспечивают повышение дальности составного акустического ка нала до единиц км и возможность съема информации злоумыш-

ленником за пределами контролируемой зоны. Закладное устройство как ретранслятор является более надежным элементом канала утечки, чем побочное излучение сигнала, так как процесс образования канала утечки информации на основе закладки управляем злоумышленником.

Другой способ повышения дальности акустического канала утечки информации обеспечивается составным **акусто-оптическим каналом утечки информации**. Схема его указана на рис. 6.7.


*Рис. 6.7.* Структура акусто-оптического канала утечки информации

Составной акусто-оптический канал утечки информации образуется путем съема информации с плоской поверхности, колеблющейся под действием акустической волны с информацией, лазерным лучом в ИК-диапазоне. В качестве такой поверхности используются стекла закрытого окна в помещении, в котором циркулирует секретная (конфиденциальная) информация. Теоретически рассматривается возможность съема информации с внешней стороны стены помещения, но данных о реализации подобной идеи нет.

С целью образования оптического канала стекло облучается лазерным лучом с внешней стороны, например, из окна противоположного дома. Луч лазера в ИК-диапазоне для посторонних лиц и находящихся в помещении невидим. В месте соприкосновения лазерного луча со стеклом происходит акустооптическое преобразование, т. е. модуляция лазерного луча акустическими сигналами от разговаривающих в помещении людей.

Модулированный лазерный луч принимается оптическим приемником аппаратуры лазерного подслушивания, преобразуется в электрический сигнал, который усиливается, фильтруется, демодулируется и подается в головные телефоны для прослушивания оператором или в аудиомагнитофон для консервации.

## 6.6. Оптические каналы утечки информации

Структура оптического канала утечки информации имеет вид, показанный на рис. 6.8.

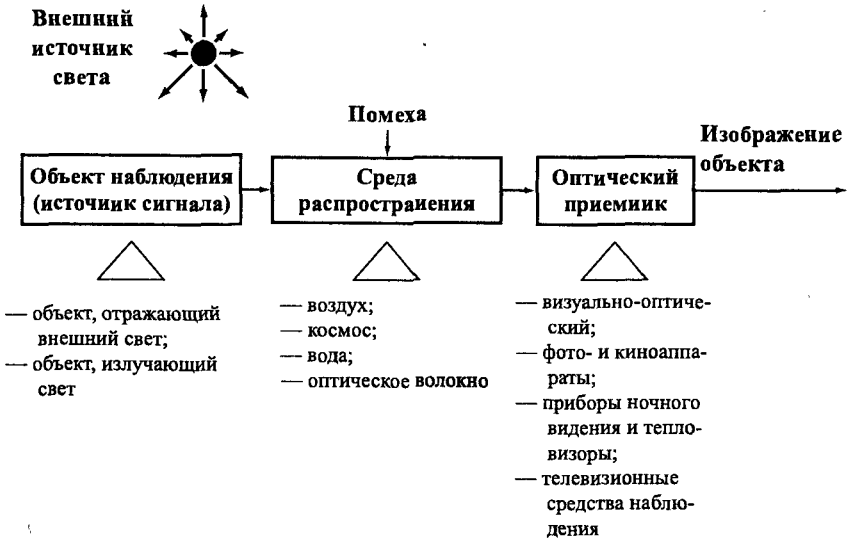



*Рис. 6.8.* Структура оптического канала утечки информации

В общем случае источником оптического сигнала является объект наблюдения, который излучает сигнал или переотражает свет другого, внешнего источника. Отражательная способность объектов наблюдения зависит от длины волны падающего света и спектральных характеристик поверхности объекта наблюдения. Отражательная способность ряда природных фонов (травы, листы и др.) и биологических объектов возрастает в несколько раз при смещении длины волны падающего света в область более длинных волн, а для неживых объектов она меняется мало в широком диапазоне длин волн.

Мощность источника светового сигнала характеризуется величиной **светового потока** в люменах (лм). Световой поток излучающего объекта наблюдения определяется как произведение силы излучаемого света на телесный угол в стерадианах (ср), в пределах которого распространяется свет в направлении на оптический приемник. **Яркость излучения** измеряется в канделлах на м$^2$ или

см$^2$. Яркость приблизительно около 1 кд/см$^2$ создают горящая свеча и голубое небо днем.

Если объект наблюдается в отраженном свете, то создаваемый им световой поток равен произведению освещенности объекта на площадь проекции объекта на плоскость, перпендикулярную направлению наблюдения. Освещенность измеряется в люксах (лк).

Источники оптических сигналов в видимом и ИК-диапазонах оптических каналов утечки информации характеризуются следующими показателями:

- диапазоном длин волн — 0,4–0,76 мкм в видимом диапазоне, 0,76–3 мкм — в ближнем, 3–6 мкм — в среднем, 8–14 мкм — в дальнем ИК-диапазонах;
- освещенностью объектов наблюдения внешним (солнечным) светом — $10^{-5}$–$10^5$ люкс (лк).

Основным и наиболее мощным внешним источником света, освещающим объекты наблюдения в дневное время, является Солнце. При температуре поверхности около 6000° С Солнце излучает огромное количество энергии в достаточно широкой полосе — от ультрафиолетового до инфракрасного (0,17–4 мкм). Максимум солнечного излучения приходится на 0,47 мкм, в ультрафиолетовой части оно резко убывает, в инфракрасной области зависимость уровня излучения от длины волны регистрируется в виде широкой и пологой кривой.

При прохождении через атмосферу солнечные лучи взаимодействуют с содержащимися в ней молекулами газов, частицами пыли, дыма, кристалликами льда, каплями воды. В результате такого взаимодействия часть солнечной энергии поглощается, другая — рассеивается.

Процессы рассеяния и поглощения солнечной энергии уменьшают интенсивность солнечной радиации на поверхности Земли и меняют спектр солнечного света, освещающего наземные объекты. В кривой излучения этого света, описывающей интенсивность излучения в зависимости от длины волны, появляются участки поглощения и пропускания. Излучения длиной менее 0,27 полностью поглощаются озоном. Поэтому уменьшение концентрации озона в верхних слоях атмосферы в так называемых «озоновых дырах» создает серьезную опасность облучения людей мощным ультрафиолетовым светом.

Атмосферное рассеяние света уменьшает прямую солнечную радиацию и повышает рассеянное (диффузное) излучение атмосферы. Рассеяние в коротковолновой части спектра сильнее, чем в длинноволновой. Особенно заметно оно в голубой и ультрафиолетовой областях, Поэтому небо имеет голубой цвет. Интенсивность рассеяния солнечного света в ближнем инфракрасном диапазоне незначительная.

Задымленность приповерхностного слоя атмосферы мало влияет на излучения в ближнем ИК-диапазоне, если размеры твердых частиц дыма в атмосфере не превышают 1 мкм. Туман и облака очень сильно рассеивают ИК-излучение в этом интервале длин, так как водяные капли имеют размер около 4 мкм. Молекулярное и аэрозольное рассеяние солнечного света вызывает ее свечение в атмосфере, которое называют **дымкой**. Рассеянное излучение создает освещенность теневых участков земной поверхности, увеличивая их относительную яркость.

Облачность существенно влияет на суммарную освещенность. Наличие облачности высоких ярусов, не закрывающих солнечный диск, повышает рассеянное излучение и при сохранении значения прямой освещенности увеличивает ее суммарную величину на 20–30% по сравнению с освещенностью при безоблачном небе. Низкая облачность так же, как и тени облаков, снижает в зависимости от высоты Солнца суммарную освещенность в 2–5 раз. При снежном покрове и облачности многократное отражение ими излучения повышает суммарную освещенность, особенно в теневых участках.

Освещенность в дневное время земной поверхности Солнцем составляет в зависимости от его высоты, облачности атмосферы $10^1$–$10^5$ лк. С движением Солнца к горизонту Земли, когда зенитное расстояние между ними достигает максимума, освещенность Солнцем уменьшается до 10 лк. При этом изменяется спектр солнечного света. Так как при прохождении толщи атмосферы синие и фиолетовые лучи ослабляются сильнее, чем оранжевые и красные, максимум излучения Солнца смещается в красную область цвета. С заходом Солнца за горизонт и наступлением сумерек освещенность убывает вплоть до наступления астрономических сумерек, за которыми следует наиболее темное время суток — ночь.

Освещенность в лунную ночь при безоблачном небе, когда так называемую **естественную ночную освещенность (ЕНО)** созда-

ет отраженный от Луны солнечный свет, составляет около 0,3 лк. Величина ЕНО света Луны в течение месяца меняется приблизительно в 100 раз в зависимости от взаимного положения Луны, Солнца и Земли. Лунный месяц разделяется по уровню освещенности на четыре части, каждая длительностью около недели.

Источниками излучения в безлунную ночь при безоблачном небе, называемого **звездным светом**, являются солнечный свет, отраженный от планет и туманностей, свет звезд, а также свечение кислорода и азота в верхних слоях атмосферы на высоте 100–300 км. Освещенность поверхности Земли звездным светом составляет в среднем 0,001 лк.

В инфракрасном диапазоне мощность излучения объекта зависит от температуры тела или его элементов, мощности падающего на объект света и коэффициента отражения объекта в этом диапазоне. Коэффициент теплового излучения для реальных объектов не постоянен по спектру и определяется в соответствии с законом Кирхгофа отношением спектральной плотности энергетической яркости объекта к спектральной плотности энергетической яркости абсолютно черного тела, которое обладает максимумом энергии теплового излучения по сравнению со всеми другими источниками при той же температуре.

Средняя температура поверхности Земли близка к 17° по Цельсию. Максимум ее теплового излучения приходится на длину волны, равную приблизительно 9,7 мкм. Объекты под действием солнечной радиации в течение дня по-разному отдают накопленное тепло в окружающее пространство. Различия в температуре излучения могут рассматриваться как демаскирующие признаки.

Объекты могут иметь собственные источники тепловой энергии, например высокотемпературные элементы машин, дизельэлектростанции и др., температура которых значительно выше температуры фона. Максимум теплового излучения таких объектов смещается в коротковолновую область, что является их демаскирующим признаком.

Объект наблюдения в оптическом канале утечки информации может рассматриваться одновременно как источник информации и источник сигнала, так как световые лучи, несущие информацию о видовых признаках объекта, представляют собой отраженные объектом лучи внешнего источника или его собственные излучения.

Отраженный от объекта свет содержит информацию о внешнем виде (видовых признаках) объекта, а излучаемый объектом свет — о параметрах излучений (признаках сигналов). Запись информации производится в момент отражения падающего света путем изменения его яркости и спектрального состава. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения.

Освещенность E некоторых объектов наблюдения на улице и в помещении указана в табл. 6.7.

*Таблица 6.7*

| *Объект наблюдения на улице* | *E, лк* | *Объект наблюдения в помещении* | *E, лк* |
|---|---|---|---|
| Яркий солнечный свет | $10^4$–$10^5$ | Офис | 200–500 |
| Пасмурный день | $10^2$–$10^3$ | Магазин | 75–300 |
| Сумерки | 1–10 | Коридор | 75–200 |
| Полная луна | 0,1–1 | Производственные помещения для:<br>— грубой работы;<br>— работы средней сложности;<br>— тонкой работы;<br>— очень тонкой работы | <br><br>40–100<br>80–300<br><br>150–1000<br>300–5000 |
| Пасмурная ночь | 0,1–0,01 | Жилые помещения | 40–150 |
| Безлунная ясная ночь | $10^{-3}$–$10^{-2}$ | Переходы и лестницы | 15–30 |
| Безлунная пасмурная ночь | $10^{-5}$–$10^{-4}$ | Заводские дворы ночью | 3–15 |

В видимом диапазоне мощность излучения определяется в подавляющем большинстве случаев мощностью отраженного света и содержащихся в объекте искусственных источников света. Например, габариты автомобиля в ночное время обозначаются включенными фонарями красного цвета, укрепленными по краям автомобиля. Собственные электромагнитные излучения в видимом диапазоне объект наблюдения или его элементы излучают при

высокой температуре. В ближней (0,76–3 мкм) и средней (3–6 мкм) диапазонах ИК-излучения объектов значительно меньше мощности отраженного от объекта потока солнечной энергии. Однако с переходом в длинноволновую область ИК-излучения мощность теплового излучения объектов может превышать мощность отраженной солнечной энергии.

**Среду распространения** в оптическом канале утечки информации образует:

- безвоздушное (космическое) пространство;
- атмосфера;
- вода;
- оптические волокна.

Оптический канал утечки информации, среда распространения которого содержит участки безвоздушного пространства, возникает при наблюдении за наземными объектами с космических аппаратов. Граница между космическим пространством и атмосферой достаточно условна. В приземном космическом пространстве на высоте 100–200 км существуют еще остатки газов, тормозящие низкоорбитальные космические аппараты.

Сложный состав атмосферы вызывает неравномерность (избирательность) ее амплитудно-частотной характеристики как среды распространения. Участки в ней с малым затуханием называются **окнами прозрачности**. Диапазон зрения человека соответствует одному из наиболее широких и благоприятному для зрения окну прозрачности, что подтверждает земное происхождение человека.

В общем случае прозрачность атмосферы зависит от соотношения длины проходящего сквозь нее света и размеров взвешенных в атмосфере частиц. Если размеры частиц соизмеримы с длиной волны света (больше половины длины волны) или больше, то пропускание значительно ухудшается. Поэтому уровень пропускания меняется в зависимости от длины световой волны.

В видимой области прохождению света препятствуют абсорбирующие фотоны света молекулы кислорода и воды. Относительный коэффициент пропускания видимого света составляет около 60%. В ближней ИК-области пропускание несколько большее — до 70%. Адсорбентом в этой области являются пары воды. В средней ИК-области, в диапазоне 3–4 мкм, пропускание достигает почти 90%.

Высокое пропускание имеет довольно обширный участок в дальней ИК-области (с 8 до 13 мкм). Абсорбентом в нем являются молекулы кислорода и воды, а также углекислого газа и озона в атмосфере.

Прозрачность атмосферы среды распространения света оценивается **метеорологической дальностью видимости**. Метеорологическая видимость даже в окнах прозрачности зависит от наличия в атмосфере взвешенных частиц пыли и влаги, образующих мглу и туман, капелек и кристаллов воды в виде дождя и снега, а также аэрозолей и дымов, содержащих твердые частицы. Все это вызывает замутнение атмосферы и ухудшает видимость. Под метеорологической дальностью видимости понимается предельно большое расстояние, начиная с которого при данной прозрачности атмосферы в светлое время суток абсолютно черный предмет с угловыми размерами 20' × 20' сливается с фоном у горизонта и становится невидимым. Значения метеорологической дальности видимости, видимости в баллах и визуальной оценки замутненности атмосферы приведены в табл. 6.8 [7].

*Таблица 6.8*

| *Метеорологическая дальность видимости, км* | *Оценка видимости, баллы* | *Визуальная оценка замутненности атмосферы* |
|---|---|---|
| Менее 0,05 | 0 | Очень сильный туман |
| 0,05–0,2 | 1 | Сильный туман |
| 0,2–0,5 | 2 | Умеренный туман |
| 0,5–1,0 | 3 | Слабый туман |
| 1,0–2,0 | 4 | Очень сильная дымка (очень плохая виднмость) |
| 2,0–4,0 | 5 | Сильная дымка (плохая видимость) |
| 4,0–10,0 | 6 | Умеренная дымка (посредственная видимость) |
| 10,0–20,0 | 7 | Слабая дымка (удовлетворительная видимость) |
| 20,0–50,0 | 8 | Хорошая видимость |
| Более 50,0 | 9 | Исключительно хорошая видимость |
| Более 200 | 10 | Чистый воздух |

Показатели метеорологической дальности атмосферы в конкретном районе регулярно определяются на станциях метеорологической службы и в метрах или в баллах передаются радиостанциями пользователям этой информации, в том числе водителям автотранспорта.

Если объект наблюдения и наблюдатель находятся на Земле, то протяженность канала утечки зависит не только от состояния атмосферы, но и ограничивается влиянием кривизны Земли. Дальность прямой видимости $D_{пв}$ в км с учетом кривизны Земли можно рассчитать по формуле:

$$D_{пв} = 3{,}57(\sqrt{h_о} + \sqrt{h_н}),$$

где $h_о$ — высота размещения объекта над поверхностью Земли в м; $h_н$ — высота расположения наблюдателя над поверхностью Земли в м.

Например, для $h_о = 3$ м и $h_н = 5$ м $D_{пв} = 14$ км, что меньше метеорологической дальности при хорошей видимости. Эта формула не учитывает неровности поверхности Земли, растительность и различные инженерные сооружения (деревья, башни, высотные здания и т. д.), создающие препятствия для света.

Так как параметры источников сигналов и среды распространения зависят от значений спектральных характеристик носителя информации, то протяженность оптического канала утечки ее в видимом и ИК-диапазонах может существенно различаться.

Однако в общем случае потенциальные оптические каналы утечки информации имеют достаточно устойчивые признаки. Типовые варианты оптических каналов утечки информации приведены в табл. 6.9.

*Таблица 6.9*

| *Объект наблюдения (источник оптического сигнала)* | *Среда распространения* | *Оптический приемник* |
|---|---|---|
| *1* | *2* | *3* |
| Документ, продукция в помещении | Воздух<br>Воздух + стекло окна | Глаза человека + бинокль, фотоаппарат |

| 1 | 2 | 3 |
|---|---|---|
| Продукция во дворе, на машине, на платформе | Воздух<br>Атмосфера + безвоздушное пространство | То же<br>Фото, ИК, телевизионная аппаратура на КА |
| Человек в помещении, во дворе, на улице | Воздух<br>Воздух + стекло | Глаза человека + бинокль, фото-, кино-, телевизионная аппаратура |

До недавнего времени атмосфера и безвоздушное пространство были единственной средой распространения световых волн. С разработкой волоконно-оптической технологии появились направляющие линии связи в оптическом диапазоне, которые в силу больших их преимуществ по сравнению с традиционными электрическими проводниками рассматриваются как более совершенная физическая среда для передачи больших объемов информации. Линии связи, использующие оптическое волокно — волоконно-оптические линии связи (ВОЛС), устойчивы к внешним помехам, имеют малое затухание, долговечны, обеспечивают значительно большую безопасность передаваемой по волокну информации.

Волокно представляет собой нить диаметром около 100 мкм, изготовленную из кварца на основе двуокиси кремния. Волокно состоит из сердцевины (световодной жилы) и оболочки из оптически менее плотного кварца. Значения показателей преломления (отношений скорости света в вакууме к скорости распространения света в среде) жилы и оболочки выбираются такими, чтобы обеспечить полное отражение света, распространяющегося по световодной жиле, от границы между жилой и оболочкой. Предельный угол полного отражения света (угол падения света на границу раздела среды, при равенстве и превышении которого наблюдается полное отражение от него) определяется из соотношения $\alpha = \arcsin(n_ж / n_o)$, где $n_ж$ и $n_o$ — показатели преломления жилы и оболочки (рис. 6.9).

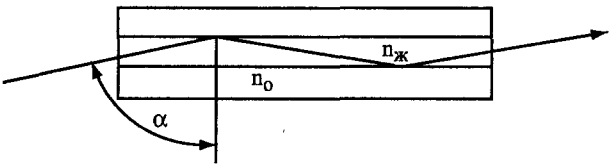



*Рис. 6.9.* Распространение света в оптическом волокне

Волокно, у которого сердцевина имеет постоянный показатель преломления света, называется **ступенчатым**. Если показатель преломления жилы меняется, то волокно называется **градиентным**.

Для передачи оптических сигналов применяются два вида волокна: **одномодовое** и **многомодовое**. В одномодовом волокне световодная жила имеет диаметр порядка 8–10 мкм, по которой может распространяться один луч (одна мода) (рис. 6.10 а)). В многомодовом волокне диаметр световодной жилы составляет 50–60 мкм, что делает возможным распространение в нем большого числа лучей (рис. 6.10 б)).

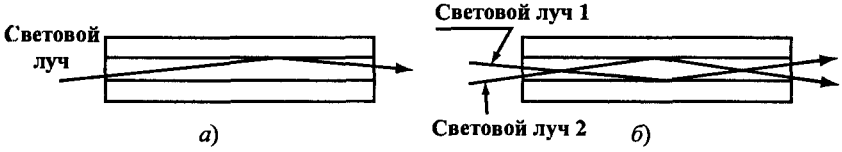



*Рис. 6.10.* Одномодовые и многомодовые оптические волокна

Оптическое волокно как среда распространения оптического канала утечки информации характеризуется двумя основными параметрами: **затуханием** и **дисперсией**. Затухание определяет потери света в результате его поглощения и рассеяния и измеряется в децибелах на километр (дБ/км). Потери на поглощение зависят от чистоты материала и длины волны света, а потери на рассеяние — от неоднородности показателя преломления. Кварц, так же как и воздух, имеет неравномерную амплитудно-частотную характеристику, с окнами прозрачности. Повышенная прозрачность кварца наблюдается в диапазонах 0,85 мкм, 1,3 мкм, 1,55 мкм и др. Поэтому в качестве носителя информации применяется свет в этих диапазонах. Лучшие образцы волокна имеют затухание порядка 0,15–0,2 дБ/км, разрабатываются еще более «прозрачные» волокна с теоретическими значениями затухания порядка 0,02 дБ/км для волны длиной 2,5 мкм. При таком затухании сигнала могут передаваться на расстояние в сотни км без ретрансляции (регенерации), что существенно превышает длину аналогичных линий связи на электрических проводах.

Так как лазер, который используется в качестве источника света для оптических каналов связи, излучает не идеальное монохром-

ное колебание, а некоторый спектр длин волн, то спектральные составляющие оптического сигнала распространяются по светопроводу с разными фазовыми скоростями, которые зависят от показателя преломления. В результате этого происходит разброс — **дисперсия** моментов прихода в точку приема спектральных составляющих сигнала. Она приводит к искажению (расширению) формы сигнала при его распространении в волокне, что ограничивает дальность передачи и верхнее значение частоты спектра сигнала. Дисперсия волокна оценивается величиной увеличения длительности оптического сигнала $\Delta\tau$ или эквивалентной полосы частоты пропускания $\Delta f$ в МГц на один км длины. При этом $\Delta\tau \approx 1 / \Delta f$.

Волокна объединяют в волоконно-оптические кабели, покрытые защитной оболочкой. По условиям эксплуатации кабели подразделяются на **монтажные, станционные, зоновые** и **магистральные**. Кабели первых двух типов используются внутри зданий и сооружений. Зоновые и магистральные кабели прокладываются в колодцах кабельных коммуникаций, в грунтах, на опорах, под водой.

Малые размеры жилы световолокна и необходимость обеспечения центрирования жил и параллельности поверхностей торцов волокон при их соединении создают определенные трудности при коммутации и ремонте ВОЛС по сравнению с электрическими проводами. Для соединения волокон с приемно-передающей аппаратурой используются **коннекторы** (соединители) различных типов с накидной гайкой и защелками-фиксаторами. Затухание оптического сигнала в коннекторах составляет доли дБ. Волокна сращиваются путем сварки, механического соединения с помощью специальных пластиковых устройств — «сплайсов», представляющих соединения в прецизионной втулке с гелем, оптические свойства которого совпадают с оптическими свойствами волокна.

Хотя возможность утечки информации из волоконно-оптического кабеля существенно ниже, чем из электрического, но при определенных условиях такая утечка возможна. Для съема информации теоретически можно разрушить защитную оболочку кабеля, найти нужное оптическое волокно, прижать фотодетектор приемника к очищенной площадке волокна и изогнуть волокно на угол, при котором не обеспечивается полное отражение оптического луча внутри волокна и часть световой энергии попадает на фотодетек-

тор приемника. Практически информацию из оптического волокна добывают в местах соединения кабеля с техническими средствами или участков кабеля друг с другом. Во-первых, в местах соединения трудно исключить излучение света в окружающее пространство из-за смещения соединяемых волокон, наличия зазора между ними, непараллельности торцевых поверхностей волокон, углового рассогласования осей волокон и различия в их диаметрах. Во-вторых, в этих местах реален доступ к волоконно-оптическому кабелю и оперативная замена штатных коннекторов на коннекторы с отводом части световой энергии к фотодетектору оптического приемника злоумышленника.

В качестве **оптических приемников** оптических каналов утечки информации используются:

- оптические приборы, расширяющие возможности зрения наблюдателя (бинокли, зрительные трубы, специальные телескопы и др.);
- фото- и киноаппараты, видеокамеры, консервирующие наблюдаемое изображение;
- телевизионные камеры, позволяющие передавать движущееся изображение на сколь угодно большое расстояние;
- приборы ночного видения, преобразующие невидимое глазом инфракрасное изображение в видимое;
- тепловизоры, позволяющие наблюдать объект в свете его собственного теплового излучения.

Показатели оптического приемника существенно влияют на характеристики оптических каналов утечки информации. Наиболее существенные для добывания информации из них следующие:

- диапазон длин волн, воспринимаемых оптическим приемником;
- чувствительность, определяемая минимальным уровнем светового потока на входе оптического приемника, при котором на его выходе формируется изображение объекта с приемлемым для злоумышленников качеством;
- разрешающая способность, характеризующая минимальные размеры точки (пикселя) изображения;
- угол (поле) зрения, определяющий наблюдаемую часть пространства;

- величина геометрических и цветовых искажений изображения объекта наблюдения.

От этих показателей зависит возможность добывания видовых демаскирующих признаков объекта наблюдения в различных участках оптического диапазона длин волн, дальность наблюдения объекта, точность измерения демаскирующих признаков, количество объектов на изображении. Характеристики средств наблюдения рассмотрены в разд. III.

## 6.7. Радиоэлектронные каналы утечки информации

### 6.7.1. Виды радиоэлектронных каналов утечки информации

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимости функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокой достоверности добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев дезинформации);
- большого объема добываемой информации;
- оперативности получения информации вплоть до реального масштаба времени;
- скрытности перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио- и электрических сигналов, а также радиолокационное и радиотеплолокационное наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация, видовые и сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио-, радиотехническая, радиолокационная и радиотепловая разведка.

Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала (рис. 6.11).

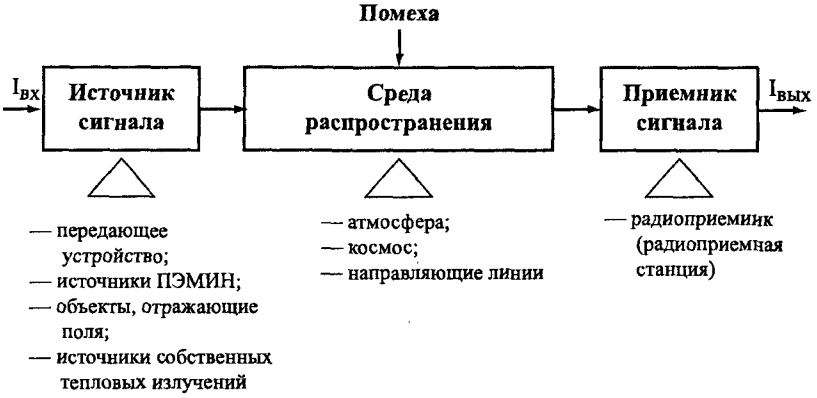



*Рис. 6.11.* Структура радиоэлектронного канала утечки информации

В радиоэлектронных каналах утечки информации источники сигналов могут быть:

- передающие устройства функциональных каналов связи;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- объекты, отражающие электромагнитные волны в радиодиапазоне;
- объекты, излучающие собственные (тепловые) электромагнитные волны в радиодиапазоне.

Радиоэлектронные каналы в зависимости от вида источников сигналов можно разделить на каналы 1 и 2-го вида. В каналах утечки **первого вида** производится перехват информации, передаваемой по функциональному каналу связи (рис. 6.12). С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала или подключается (контактно или дистанционно) к проводам соответствующего канала связи. Такой канал утечки имеет общий с функциональным каналом связи источник сигналов — передатчик и часть среды радиоканала или проводного функционального канала до точки подключения средства съе-

ма. Эта особенность иллюстрируется стрелкой распространения носителя (электрического тока) из среды распространения функционального канала связи в среду распространения канала утечки информации на рис. 6.12.

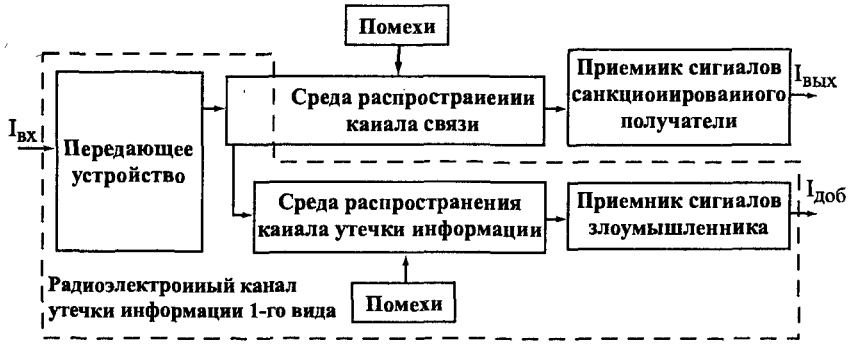



*Рис. 6.12.* Структура радиоэлектронного канала утечки информации 1-го вида

Перехватываемые сигналы передающих устройств функциональных каналов связи имеют мощность от долей Вт до миллиона Вт (МВт). Например, мощность импульсов станции дальнего радиолокационного обнаружения «Авакс» (США) составляет порядка 1 МВт в десятисантиметровом диапазоне волн. Но так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то перехватываемый сигнал имеет меньшую мощность, чем сигнал на входе приемника функционального канала связи.

**Радиоэлектронный канал утечки 2-го вида** имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов (рис. 6.13).

Передатчик сигналов этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. Такими передатчиками могут быть случайные источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают в результате акустоэлектрических

преобразований, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Предпосылки для них создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил эксплуатации, неучете полей вокруг средств или токонесущих проводов при их прокладке в здании и т. д.

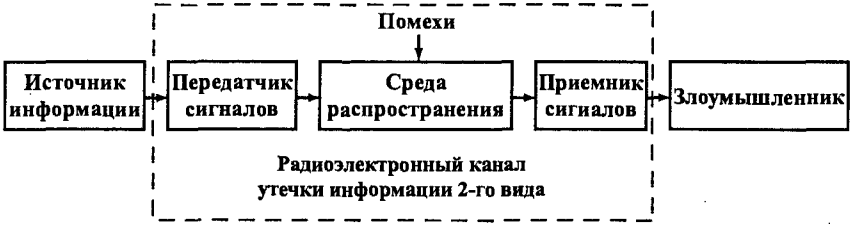



*Рис. 6.13.* Структура радиоэлектронного канала утечки информации 2-го вида

Особенностями передатчиков канала 2-го вида являются малые уровни электрических сигналов — единицы и доли мВ и мощность радиосигналов, не превышающая десятки мВт (для радиозакладок). В результате этого протяженность таких каналов невелика и составляет десятки и сотни метров. Поэтому для добывания информации с использованием такого канала утечки приемник необходимо приблизить к источнику на величину длины канала утечки или установить ретранслятор.

Средой распространения сигналов радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство (для канала 1-го вида) и направляющие — электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле — в атмосфере, в безвоздушном пространстве или по направляющим — волноводам. В приемнике производится выделение (селекция) носителя с интересующей получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации — демодуляция.

### 6.7.2. Распространение опасных электрических и радиосигналов в радиоэлектронном канале утечки информации

Среда распространения радиоэлектронных каналов утечк существенно различается для электрических и радиосигнало Электрические сигналы как носители информации могут быть ан логовыми или дискретными, их спектр может содержать частот от десятков Гц до десятков ГГц. Электрические сигналы распр страняются по **направляющим линиям связи**, связывающим ис точники и приемники сигналов как внутри организации, так внут ри населенного пункта, города, страны, земного шара в целом Способы и средства передачи электрических сигналов по прово дам рассматриваются теорией и техникой проводной связи.

Классификация направляющих электрических линий связи приведена на рис. 6.14.

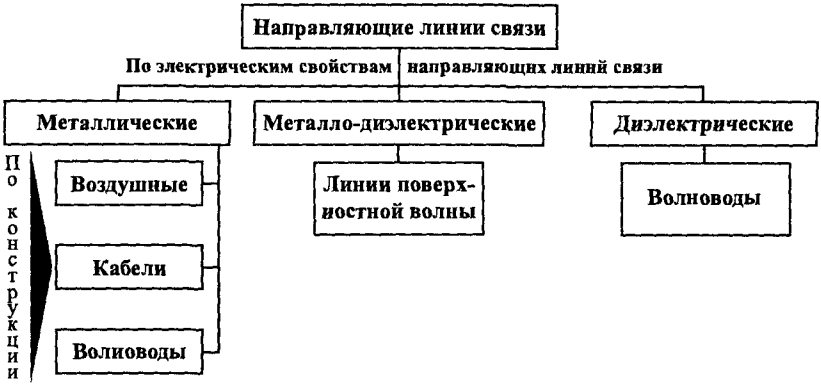



*Рис. 6.14.* Классификация направляющих линий связи

Направляющие металлические линии включают **воздушные** и **кабельные проводные линии связи** и **волноводы**.

**Воздушные линии** связи образуют провода, натянутые в воздушном пространстве между опорами. В зависимости от типа несущих конструкций они делятся на **столбовые и стоечные**. Столбовыми называются линии, несущими конструкциями которых являются деревянные или железобетонные опоры. Опорами столбовых линий служат металлические стойки, установленные, например, на крышах зданий. Для изоляции проводов воздушных

линий друг от друга и относительно земли их укрепляют на фарфоровых изоляторах. Воздушные линии имеют малый частотный диапазон и подвержены воздействию климатических факторов, например обледенению.

Более широко применяются **кабельные линии** связи. Кабельные линии связи получили доминирующее развитие при организации объектовой, городской и междугородной телефонной связи. Они составляют более 50% телефонных линий России. Наиболее распространены кабели на витой паре и коаксиальные кабели.

Витая пара относится к **симметричным кабелям** и представляет собой два изолированных провода с одинаковыми электрическими параметрами, скрученные вместе. Провода покрываются изоляционным материалом (чаще поливинилхлоридом или полиэтеленом) Тип и толщина слоя изоляционного материала определяют емкость между проводами в кабеле. Телекоммуникационные кабели могут содержать от двух до 3000 витых пар, полностью покрытых изоляционной оболочкой. Витую пару можно представить в виде электрической модели из двух сопротивлений, параллельно одному из которых подключена емкость. Входное сопротивление витой пары зависит от частоты сигнала. В диапазоне частот стандартного телефонного канала оно принимается равным 600 Ом. С увеличением частоты входное сопротивление уменьшается и на высоких частотах определяется как корень квадратный отношения распределенных индуктивности и емкости.

В **коаксиальном кабеле** один проводник концентрически расположен внутри другого проводника, имеющего форму полого цилиндра. Внутренний проводник изолируется от внешнего с помощью различных изоляционных материалов и конструкций. Для изоляции коаксиальных пар кабеля применяется полиэтилен, фторлан (фторопласт), полипропилен, резина, неорганическая изоляция. Внешний проводник высококачественной коаксиальной пары образуется фольгой и оплеткой из медной или железной сетки. Для защиты от внешних воздействий он покрывается слоем изолятора (полихлорвинила). Входное сопротивление для подсоединения радиаппаратуры обычно равно 50 Ом, а для передачи телевизионных сигналов и в связи — 75 Ом. Коаксиальный кабель имеет большую пропускную способность, чем симметричный. Стандартный ко-

аксиальный кабель 1,2/4,4 (с диаметрами внутреннего и внешнего проводников 1,2 и 4,4 мм соответственно) обеспечивает передачу 900–960 телефонных каналов на расстояние до 9 км или 3600 каналов на расстояние 1,5 км. При увеличении диаметров проводников кабеля до 2,6/9,5 число телефонных каналов для длины участка 1,5 км возрастает до 10800. Для повышения частотного диапазона требуется дальнейшее увеличение диаметра коаксиального кабеля. Например, кабель РК 50-17-51 с наружным диаметром изоляции (внешнего проводника) 17,3 мм имеет номинальный коэффициент затухания 0,012, 0,035 и 0,05 дБ/м на частотах 200, 450 и 900 Мгц соответственно.

Коаксиальный кабель на высоких частотах имеет лучшие электрические характеристики, чем витая пара. В нем практически отсутствуют перекрестные помехи и намного меньше затухание.

Несколько жил, объединенных единым изолятором в виде ленты, образуют **ленточные кабели** или **полосковые линии**.

Основными параметрами проводных линий связи являются **ширина пропускаемого** ими **спектра частот** и **собственное затухание** $Z_c = 10\lg P_{вх} / P_{вых}$, где $P_{вх}$ и $P_{вых}$ — мощность сигнала на входе и выходе цепи соответственно. Если сопротивление проводников на низких частотах (в звуковом диапазоне) определяется удельным сопротивлением материала и площадью поперечного сечения проводника, то на более высоких частотах начинается сказываться влияние **поверхностного эффекта**. Сущность его заключается в том, что переменное магнитное поле, возникающее при протекании по проводнику тока, создает внутри проводника вихревые токи, В результате этого плотность основного тока перераспределяется по сечению проводника (жилы): уменьшается в центре и возрастает на периферии. Глубина проникновения (в мм) тока в медную жилу $\theta = 67/\sqrt{f}$, где f — частота колебаний в Гц. На частоте f = 60 кГц глубина проникновения составляет приблизительно 0,3 мм, а на частоте 250 кГц — на порядок меньше, всего около 0,03 мм. Следовательно, ток с этой частотой распространяется по гипотетической тонкой медной трубке с существенно меньшей площадью сечения и, соответственно, большим сопротивлением.

На величину затухания линии влияют также электрические характеристики диэлектрика, наносимого на металлические прово-

да. За счет их удается расширить полосу пропускания линии. При передаче по воздушным линиям со стальными проводами ширина пропускания составляет около 25 кГц, с медными проводами — до 150 кГц, по симметричным кабелям — до 600 кГц. Расширению спектра частот, передаваемых по симметричным цепям, препятствуют возрастающие наводки. Например, удовлетворительным для телефонных линий считается значение переходного затухания порядка 60–70 дБ.

**Металлические волноводы** представляют собой трубы прямоугольного или круглого сечения, внутри которых может распространяться электромагнитное поле от излучателя, установленного в торце одной из сторон волновода. Волноводы применяются для передачи электромагнитного поля с длиной волны короче 10–15 см. Отражаясь от внутренней поверхности волновода, электромагнитное поле концентрируется в волноводе и при движении повторяет его изгибы. С целью уменьшения затухания электромагнитного поля внутренние стенки волновода покрывают тонким слоем серебра. Кроме медных и алюминиевых находят применение волноводы из пластических масс с металлизированными изнутри стенками.

Другие типы направляющих линий, указанные на рис. 6.14, представляют собой разновидности волноводных линий с иными физическими процессами. В **металло-диэлектрических линиях** связи электромагнитное поле распространяется в виде поверхностной волны вдоль металлической ленты или цилиндрического провода с ребристой поверхностью. Энергия электромагнитного поля концентрируется в пространстве, окружающем такой волновод, затухая по мере удаления от него. Недостатком такого волновода является паразитное излучение в эфир электромагнитного поля.

Для передачи сантиметровых и миллиметровых волн могут служить **диэлектрические волноводы**, в которых поверхностью раздела, направляющей волну, служит внутренняя поверхность диэлектрического стержня волновода. Диэлектрические волноводы чувствительны к внешним воздействиям и создают дополнительные потери, связанные с просачиванием энергии за пределы волновода, что затрудняет их практическое применение.

Основным носителем информации в радиоэлектронном канале является электромагнитное поле.

**Электромагнитное поле** представляет форму движения материи в виде взаимосвязанных колебаний электрического и магнитного полей. Электромагнитное поле возникает при протекании по проводам источника радиосигнала электрического тока переменной частоты и распространяется с конечной скоростью в окружающем пространстве. Векторы напряженности электрического и магнитного полей взаимно перпендикулярны и перпендикулярны направлению распространения электромагнитной волны. Электромагнитная волна характеризуется **частотой колебания, мощностью и поляризацией**. По частоте электромагнитные волны классифицируются в соответствии с Регламентом радиосвязи, утвержденным на Всемирной административной конференции в Женеве в 1979 г. (табл. 6.10).

*Таблица 6.10*

| *Диапазон длин волн* | *Наименование волн* | *Обозначение и наименование частот* | *Диапазон частот* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| > 100 км | – | ELF — чрезвычайно низкие | Доли Гц–3 кГц |
| 10–100 км | Мириаметровые | VLF(ОНЧ) — очень низкие | 3–30 кГц |
| 1–10 км | Километровые (длинные) | LF(НЧ) — низкие | 30–300 кГц |
| 100–1000 м | Гектаметровые (средние) | MF(СЧ) — средние | 300–3000 кГц |
| 10–100 м | Декаметровые (короткие) | HF(ВЧ) — высокие | 3–30 МГц |
| 1–10 м | Метровые | (ОВЧ) — очень высокие | 30–300 МГц |
| 10–100 см | Дециметровые | UHF(УВЧ) — ультравысокие | 300–3000 МГц |
| 1–10 см | Сантиметровые | SHF(СВЧ) — сверхвысокие | 3–30 ГГц |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| 1–10 мм | Миллиметровые | EHF(КВЧ) — крайне высокие | 30–300 ГГц |
| 0,1–1 мм | Децимиллиметровые | ГВЧ — гипервысокие | 300–3000 ГГц |

*Примечание.* Электромагнитные волны длиной менее 10 м называют также ультракороткими волнами (УКВ).

Поляризация электромагнитной волны определяется направлением вектора напряженности электрического поля. Если вектор электрического поля лежит в вертикальной плоскости, то поляризация вертикальная, когда он находится в горизонтальной плоскости, то — горизонтальная. Промежуточное положение характеризуется углом поляризации между плоскостями поляризации и распространения. **Плоскостью поляризации** называется плоскость, в которой находятся вектора электрического поля и вектор распространения электромагнитной волны.

**Мощность излучения** электромагнитного поля тем выше, чем ближе частота колебаний в распределенном контуре, образованном индуктивностью проводников и распределенной емкостью между ними и землей, к частоте сигнала. Эффективное преобразование энергии электрических сигналов в электромагнитную волну выполняется **антеннами**.

Характер поляризации электромагнитной волны зависит от конструкции и расположения излучающих элементов антенны. Несоответствие поляризации электромагнитной волны пространственной ориентации элементов приемной антенны, в которых наводятся электрические заряды, приводит к уменьшению величины этих зарядов.

Радиоволны в зависимости от характера распространения делятся на **земные (поверхностные), прямые, тропосферные** и **ионосферные (пространственные)**.

**Земными** называются радиоволны, которые распространяются в непосредственной близости от поверхности Земли и частично огибают ее поверхность в результате дифракции. **Прямыми** назва-

ны радиоволны, распространяющиеся прямолинейно в атмосфере и космосе.

Радиоволны, которые распространяются в тропосфере — приземной неоднородной области атмосферы не выше 10–12 км от поверхности Земли, называются **тропосферными**. В тропосфере происходит рассеивание, а также частичное искривление траектории и отражение радиоволн от неоднородностей тропосферы.

**Ионосферными** называют радиоволны, распространяющиеся в результате преломления их в ионосфере и отражений от земной поверхности. Ионосферу образуют ионизированные под действием ультрафиолетового излучения Солнца верхние слои атмосферы. Концентрация свободных электронов в ионосфере меняется по высоте. В зависимости от концентрации свободных электронов и, соответственно, положительно заряженных ионов ионосферу условно делят на слои — D, E, $F_1$ и $F_2$. Наименьшая концентрация имеет место в слое D, наибольшая — в слое $F_2$. Состояние ионосферы непрерывно меняется, оно зависит от времени суток, времени года и солнечной активности, которая имеет 11-летний цикл изменения.

Слой D располагается до высоты примерно 60 км. В ночные часы в слое D преобладает рекомбинация электронов, ионизация уменьшается или исчезает. Слой E расположен на высоте 100–120 км и менее зависит от времени суток, а слои $F_1$ и $F_2$ занимают области на высоте примерно 160–400 км, причем ночью слой $F_1$ исчезает.

В ионосфере происходит преломление, отражение и поглощение радиоволн. Преломление радиоволн обусловлено изменениями диэлектрической проницаемости, и, следовательно, показателя преломления по высоте слоев. По мере распространения радиоволн от наземного источника через более высоко расположенные слои показатель преломления уменьшается, траектория электромагнитной волны искривляется и при определенных условиях волна возвращается на Землю.

Преломление радиоволн на той или иной высоте ионосферы зависит от частоты радиоволн и угла их падения на слой. При прочих равных условиях, чем больше угол падения волны, отсчитываемый от вертикальной линии в точке падения, тем более пологая

траектория луча в ионосфере и тем меньшая электронная концентрация потребуется для возвращения луча на Землю. Минимальное значение угла падения, при котором еще возможно отражение радиоволн от ионосферы, называется **критическим**. При угле падения, меньшем критического, радиоволны проходят через ионосферу не отразившись.

Так как коэффициент преломления уменьшается с увеличением частоты, то длинные волны преломляются сильнее, чем короткие, а для УКВ преломление недостаточно для возвращения волн на Землю и они уходят в космическое пространство. Наивысшая частота, при которой электромагнитная волна еще может возвратиться на Землю, называется **максимально применимой частотой**. Но значение этой частоты неоднозначно вследствие зависимости ее от угла падения. Поэтому вводят понятие **критической частоты**, которая является максимально применимой частотой при угле падения 0 градусов. Из определения следует, что эта частота представляет собой низшую из всех максимально применимых частот.

За счет многократного преломления радиоволн в ионосфере и отражения от земной поверхности электромагнитная волна может распространяться на большие расстояния, вплоть до огибания Земли. Но при таком распространении волны на земной поверхности возникают зоны молчания, в которые не попадают отраженные от ионосферы электромагнитные волны. В зонах приема происходит интерференция волн, прошедших разный путь от излучателя и имеющих, следовательно, различные фазы. Случайный характер изменения фаз приводит к случайному изменению амплитуды результирующей волны, которое называется **замиранием** или **федингом**.

Степень поглощения радиоволн в атмосфере увеличивается при повышении плотности ионизации, частоты колебания и пути, проходимой радиоволной в ионосфере. Зимой, когда концентрация электронов в связи с понижением солнечной радиации уменьшается, поглощение радиоволн снижается и дальность распространения увеличивается.

В зависимости от частоты колебания радиоволн характер их распространения имеет следующие особенности.

1. Километровые (длинные) волны подвержены дифракции, сравнительно слабо поглощаются земной поверхностью и могут распространяться поверхностным лучом на расстояние до 3000 км. В ионосфере они затухают сильнее, но могут отражаться от слоя Е и распространяться пространственным лучом на большее расстояние. К преимуществам электромагнитной волны в этом диапазоне как носителя информации относится, кроме большой дальности распространения, сравнительное постоянство напряженности поля в пункте приема в течение суток и года, что обеспечивает устойчивость связи. Эти волны применяются также для связи под водой, где сильно затухают волны более высоких частот.

Недостатком длинноволновой радиолинии является плохая излучательная способность антенн даже при больших размерах, достигающих несколько сотен метров, высокий уровень атмосферных и промышленных помех и малая пропускная способность.

2. Гектаметровые (средние) волны могут распространяться поверхностным и пространственным лучами. Энергия средних волн поглощается земной поверхностью сильнее, чем длинноволновых, поэтому дальность связи поверхностным лучом составляет примерно 500–1500 км. Однако для средних волн создаются более благоприятные условия распространения пространственным лучом, для которого прием сигналов возможен до 4000 км.

Условия распространения средних волн существенно изменяются в зависимости от времени суток. В ночные часы за счет преломления в ионосфере дальность распространения выше, чем в дневные, когда преобладают поверхностные волны. В этом диапазоне наблюдаются замирания в результате интерференции земных и поверхностных волн или пространственных волн с различными путями распространения, высокий уровень атмосферных и промышленных помех. Антенны в среднем диапазоне по устройству в основном такие же, как и антенны в длинноволновом, но в силу большей близости их геометрических размеров к длинам волн имеют больший коэффициент усиления. Радиоволны в этом диапазоне используются для радиовещания и связи, на флоте и в авиации.

3. При распространении коротких волн дальность поверхностного луча невелика из-за резкого возрастания поглощения энергии землей. Поле в точке приема создается в основном за счет преломления в различных слоях ионосферы. В результате флюктуа-

ции плотности и высоты слоев и взаимодействия лучей на коротких волнах, как правило, наблюдаются глубокие замирания и даже полное пропадание связи в течение единиц и десятков секунд.

Для обеспечения круглосуточной связи в условиях суточного изменения ионосферы необходимо производить периодическую смену частот. Определение оптимальных частот производится специальными службами наблюдения за ионосферой по результатам вертикального и вертикально-наклонного зондирования ее радиоимпульсами. Наиболее благоприятные условия прохождения волн днем чаще складываются на волнах в интервале 10–25 м, а ночью — 35–70 м.

В диапазоне коротких волн на напряженность поля и характер ее изменения в точке приема влияют другие явления, такие как «вспышки» на Солнце, рассеяние волн на мелких неоднородностях ионосферы, поворот плоскости поляризации.

Достоинством коротких волн является возможность обеспечения связи на очень большие расстояния при сравнительно малых мощности передатчика и габаритах антенны, а также малое влияние атмосферных и промышленных помех. Они применяются для связи, радионавигации, радиовещания и радиолюбителями.

4. В диапазоне ультракоротких (метровых и более коротких) волн практически отсутствует дифракция. Поэтому они распространяются в пределах прямой видимости, в том числе отражаясь от земли и тропосферы с потерей части энергии на поглощение. Радиоволны в этих диапазонах являются основными носителями информации в сетях телекоммуникаций в силу следующих особенностей:

- имеют широкий частотный диапазон (см. табл. 6.10), обеспечивающий возможность передачи большого объема информации, в том числе путем использования широкополосных каналов;
- низкий уровень атмосферных и промышленных помех, позволяющих использовать приемные устройства с высокой чувствительностью, что повышает дальность приема;
- слабое влияние станционных помех на работу других радиосистем вследствие ограниченности их радиуса видимости;
- возможность создания небольших антенн с узкой диаграммой направленности, позволяющих осуществлять радиосвязь при относительно малой мощности передающих устройств.

Основной недостаток радиоволн рассматриваемого диапазона — существенно большее поглощение их в атмосфере, в том числе природными осадками (дождем, туманом, снегом, градом), особенно в миллиметровом диапазоне, и, как следствие, относительно малая дальность распространения.

Результаты сравнительного анализа характеристик радиоволн различных диапазонов приведены в табл. 6.11.

*Таблица 6.11*

| *Диапазон* | *Дальность распространения* | *Антенны* | *Уровень помех* | *Поглощение в атмосфере* |
|---|---|---|---|---|
| ДВ | Поверхностной волной — до 3 тыс. км | Громоздкие  Компактные | Высокий  Низкий | Слабое  Сильное |
| СВ | Поверхностной — до 1500 км, пространственной — до 4000 км | | | |
| КВ | Пространственной — на любое расстояние | | | |
| УКВ | Прямая видимость | | | |

Электрические сигналы как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков Гц до десятков ГГц.

Наиболее широко применяются сигналы, ширина спектра которых соответствует ширине спектра стандартного телефонного канала. Такие сигналы передают речевую информацию с помощью телефонных аппаратов и распространяются по направляющим линиям связи, связывающим абонентов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом.

Повышение дальности связи в УКВ-диапазоне обеспечивается путем:

- подъема передающей или приемной антенн с помощью инженерных конструкций (матч, башен) и аэростатов;
- ретрансляции радиосигналов с помощью наземных и космических ретрансляторов;
- использования тропосферных волн в УКВ диапазоне.

Передающие антенны на башнях устанавливаются для постоянного обеспечения связи, радио- и телевизионного вещания в городах, районах и областях. Для периодического и эпизодического приема сигналов от отдаленных источников в качестве носителей приемников сигналов используют также привязные аэростаты. Информация с них на землю передается по кабелю или радиоканалу.

Для передачи информации в УКВ-диапазонах частот на большие расстояния широко применяются ретрансляторы. С помощью наземных ретрансляторов создаются **радиорелейные линии (РРЛ)**, представляющие собой цепочку приемно-передающих станций, каждая из которых устанавливается в пределах прямой видимости соседних. Все станции РРЛ разделяются на **оконечные**, **промежуточные** и **узловые**. Оконечные радиорелейные станции располагаются в начале и конце линии. На этих станциях вводится и выделяется информация, обеспечивается распределение информации между потребителями. Промежуточные станции предназначены для ретрансляции сигналов. Узловые радиорелейные станции — это промежуточные станции, на которых происходит разветвление принимаемых сигналов по различным направлениям, выделение части передаваемой информации (например, программ телевидения) и введение новой информации.

Диапазоны частот, предназначенных для передачи информации одного вида, объединяются в радиочастотный ствол: телевизионный, телефонный и т. д. Существующие отечественные РРЛ могут содержать до 8 стволов, а один ствол, например, телефонный — до 1920 телефонных каналов. Для каждого ствола с целью исключения взаимного влияния выделяются две рабочие частоты — для передачи и приема. Принятые каждой станцией сигналы на частоте приема усиливаются и преобразуются в частоту передачи, на которой излучаются в направлении следующей станции. Радиорелейная связь обеспечивает около 30% телефонных каналов России.

Для повышения дальности в **тропосферных линиях связи** используют явление рассеяния ультракоротких радиоволн в неоднородностях тропосферы. К таким неоднородностям относятся области тропосферы с резко изменившимися значениями диэлект-

рической проницаемости. Неоднородности вызываются неравномерностью состояний различных точек тропосферы, непрерывным перемешиванием и смещением воздушных масс в результате неравномерного разогрева Солнцем различных участков поверхности Земли и слоев тропосферы. Для устойчивой тропосферной радиосвязи применяют антенны с высоким коэффициентом усиления (40–50 дБ), мощные передатчики (1–10 кВт) и высокочувствительные приемники. Тропосферные линии связи чаще всего имеют протяженность 140–500 км.

Ретрансляторы, устанавливаемые на **искусственных спутниках Земли (ИСЗ)**, наиболее широко используются для обмена информацией между абонентами, удаленными друг от друга на тысячи километров. Они являются элементами (звеньями) спутниковых систем связи, которые содержат также оконечные наземные передающие и приемные станции. Естественно, что связь возможна лишь в том случае, если спутники находятся в зоне видимости обеих земных станций. Для ретрансляции радиосигналов применяются **космические аппараты (КА)** на геостационарной (стационарной) и эллиптической орбитах, а также низкоорбитальные КА.

При распространении радиоволн в городе характер их распространения существенно искажается по сравнению с распространением на открытых пространствах за счет многочисленных переотражений от стен зданий и помещений и затухания в них. Эти обстоятельства необходимо учитывать при оценке пространственной ориентации и возможностей каналов утечки информации. Экранирующие свойства некоторых элементов здания приведены в табл. 6.12 [17].

*Таблица 6.12*

| *Тип здания* | *Ослабление, дБ на частоте* | | |
|---|---|---|---|
| | *100 МГц* | *500 МГц* | *1 ГГц* |
| Деревянное здание с толщиной стен 20 см | 5–7 | 7–9 | 9–11 |
| Кирпичное здание с толщиной стен 1,5 кирпича | 13–15 | 5–17 | 16–19 |
| Железобетонное здание с ячейкой арматуры 15 × 15 см и толщиной 160 мм | 20–25 | 18–19 | 15–17 |

Указанные в таблице данные получены для стен, 30% площади которых занимают оконные проемы с обычным стеклом. Если оконные проемы закрыты металлической решеткой с ячейкой размером 5 см, то эффективность экранирования увеличивается на 30–40 %. Экранирующие свойства кирпичных и железобетонных стен зданий в 2–3 раза выше, чем деревянных.

Многообразие природных и искусственных источников излучений в радиодиапазоне порождает проблему электромагнитной совместимости радиосигналов с определенной информацией с другими радиосигналами — помехами с совпадающими частотами. Классификация помех представлена на рис. 6.15.


*Рис. 6.15.* Классификация помех по их источникам

Естественные или природные помехи имеют земное и внеземное происхождение. Земные помехи вызываются физическими процессами в атмосфере, Земле и объектах на ее поверхности, основные из которых следующие:

- электрические грозовые разряды на частотах, как правило, менее 30 Мгц;
- разряды статического электричества в облаках и атмосферных осадках;

- резонансные электрические колебания между Землей и ионосферой;
- тепловое излучение Земли и зданий в диапазоне более 30–40 МГц;
- тепловые шумы в элементах и цепях радиоприемников.

Внеземные помехи на частотах выше 1 МГц обусловлены комбинированным излучением Галактики с дискретным и сплошным спектром. Солнце является мощным источником электромагнитных излучений, особенно в период его высокой активности, в основном на частотах выше 20 МГц. Луна, Юпитер и сверхновая звезда Кассиопея-А представляют собой дополнительные источники космических помех в УКВ-диапазонах. Другие источники естественных помех включают тепловое галактическое излучение, излучение ионизированного и нейтрального водорода и др. Земли достигают также помехи низкой интенсивности, обусловленные вспышками звезд и излучениями радиогалактик.

Обратной стороной технического прогресса является рост уровня **искусственных помех**. Наиболее интенсивные радиоизлучения создаются передающими устройствами различных радио- и радиотехнических средств (станций радиовещания и телевидения, радиолокации, радионавигации, связи и др.). В целях обеспечения их электромагнитной совместимости частоты радиодиапазонов закреплены международными соглашениями и нормативными документами между различными видами деятельности и средств.

К источникам **непреднамеренных помех**, возникающих в результате побочных физических эффектов работы технических средств, относятся различные генераторы и преобразователи электроэнергии, линии электропередач, промышленное оборудование, транспорт на электрической тяге, системы зажигания двигателей внутреннего сгорания, медицинское оборудование, сварочные аппараты, осветительные газоразрядные лампы и др.

**Преднамеренные помехи** создаются специально для подавления систем управления и связи противника в военное время и защиты своей информации от перехвата содержащих ее радиосигналов радиоэлектронными средствами добывания. Так как эффективность боевых действий в современных условиях зависит от надежности и достоверности связи в войсках и управления оружием, то подавление их мощными помехами не менее, а иногда и более

результативно, чем применение оружия. Для ведения радиоэлектронной борьбы в вооруженных силах существует специальный род войск. Электромагнитное зашумление с целью защиты информации создается также генераторами помех, размещаемых в помещениях, в которых циркулирует защищаемая информация.

По эффекту воздействия радиоэлектронные помехи делятся на маскирующие и имитирующие (рис. 6.16).


*Рис. 6.16.* Классификация помех по их характеристикам

Маскирующие помехи создают помеховый фон, на котором затрудняется или исключается обнаружение и распознавание полезных сигналов. Имитирующие помехи по структуре близки к полезным сигналам и при приеме могут ввести в заблуждение получателя. С этой целью электромагнитные колебания помех модулируются по амплитуде и частоте (фазе), изменяются параметры импульсных помех, вызывающих срыв слежения в импульсных радиолокационных станциях управления оружием и определения координат целей.

По виду сигнала помехи делятся на **флуктуационные, гармонические** и **импульсные**. Флуктуационные помехи имеют распределенный по частоте спектр и создаются коронами высоковольтных линий электропередач, лампами дневного света, неоновой рекламой, электросваркой и другими электрическими разрядами. Спектр промышленных гармонических помех локализован на частотах излучений, возникающих при нелинейных преобразованиях в промышленных установках. Импульсные помехи, возникающие, прежде всего, при замыкании и размыкании электрических контактов выключателей, характеризуются сосредоточением энергии электромагнитных излучений в короткий промежуток времени.

Так как электромагнитные волны в радиодиапазоне являются основными носителями информации, то с целью нарушения управления и связи в ходе радиоэлектронной борьбы созданы разнообразные средства генерирования помех.

По соотношению спектра помех и полезных сигналов помехи подразделяются на **заградительные** и **прицельные**. Заградительные помехи имеют ширину спектра частот, значительно превышающую ширину спектра полезного сигнала, что позволяет подавлять сигнал без точной настройки генератора помех на его частоту.

Прицельная помеха имеет ширину спектра, соизмеримую (равную или превышающую в 1,5–2 раза) с шириной спектра сигнала, и создает высокий уровень спектральной плотности мощности в полосе частот сигнала при небольшой (относительно мощности заградительной помехи) мощности передатчика помех.

Помеха изменяет демаскирующие признаки сигнала случайным образом (маскирующая помеха) или формирует демаскирующие признаки другого объекта сигнала (имитирующая помеха).

Помеха, которая зашумляет пространство, называется **пространственной**, а помеха, распространяющаяся по направляющим линиям, — **линейной**.

## 6.8. Вещественные каналы утечки информации

### 6.8.1. Общая характеристика вещественного канала утечки информации

Особенность этого канала вызвана спецификой источников и носителей информации по сравнению с другими каналами. Источниками и носителями информации в нем являются субъекты (люди) и материальные объекты (макротела и микрочастицы). Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Для более четкого описания рассматриваемого канала целесообразно уточнить состав источников и носителей информации.

Основными источниками информации вещественного канала утечки информации являются следующие:

- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;
- отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;
- отходы промышленного производства опытного и серийного выпуска продукции, содержащей защищаемую информацию в газообразном, жидком и твердом виде;
- содержащие защищаемую информацию дискеты и жесткие диски ПЭВМ, нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;
- бракованная продукция и ее элементы;
- радиоактивные материалы.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами:

- людьми (сотрудниками организаций, посетителями, представителями вторсырья и др.) и управляемыми ими техническими средствами;
- воздушными массами атмосферы;
- жидкой средой;
- излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках — в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т. д.; демаскирующие вещества — в газообразных, жидких и твердых отходах производства.

Структурная схема вещественного канала утечки информации приведена на рис. 6.17.

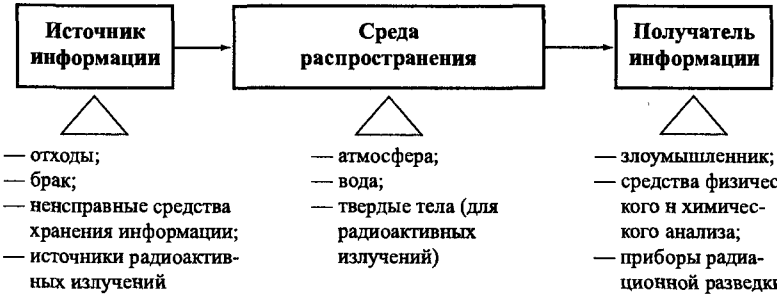



*Рис. 6.17.* Структура вещественного канала утечки информации

Приемники информации этого канала достаточно разнообразны. Это эксперты зарубежной разведки или конкурента, приборы для физического и химического анализа, средства вычислительной техники, приемники радиоактивных излучений и др.

В рамках вещественного канала ведется химическая и радиационная разведка. Демаскирующие вещества добываются в основном путем взятия проб веществ в твердой, жидкой и воздушной средах. Развиваются активные и пассивные методы и средства анализа веществ, в основном в воздушных средах. В активных методах предусматривается посылка лазерного луча к исследуемой воздушной смеси и анализ излучений результатов взаимодействия. В пассивных методах производится анализ спектра собственных излучений веществ.

Потери носителей с ценной информацией возможны при отсутствии в организации четкой системы учета ее носителей. Например, испорченный машинисткой лист отчета может быть выброшен ею в корзину для бумаги, из которой он будет уборщицей перенесен в бак для мусора на территории организации, а далее при перегрузке бака или транспортировке мусора на свалку лист может быть унесен ветром и поднят прохожим. Конечно, вероятность обеспечения случайного контакта с этим листом злоумышленника невелика, но если последний активно занимается добыванием информации, то область пространства, в котором возможен контакт, значительно сужается и вероятность утечки повышается.

Для предприятий химической, парфюмерной, фармацевтической и других сфер разработки и производства продукции, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ, возможно образование каналов утечки информации через выбросы в атмосферу газообразных или слив в водоемы жидких демаскирующих веществ.

Подобные каналы образуются при появлении возможности добывания демаскирующих веществ в результате взятия злоумышленниками проб воздуха, воды, земли, снега, пыли на листьях кустарников и деревьев, на траве и цветах в окрестностях организации.

В зависимости от розы (направлений) и скорости ветра демаскирующие вещества в газообразном виде или в виде взвешенных твердых частиц могут распространяться на расстояние в единицы и десятки км, достаточное для безопасного взятия проб злоумышленниками. Аналогичное положение наблюдается и для жидких отходов.

Конечно, концентрация демаскирующих веществ при удалении от источника убывает, но при утечке их в течение некоторого времени концентрация может превышать допустимые значения за счет накопления демаскирующих веществ в земле, растительности, подводной флоре и фауне.

Отходы могут продаваться другим предприятиям для использования в производстве иной продукции, очищаться перед сливом в водоемы, уничтожаться или подвергаться захоронению на время саморазрушения или распада. Последние операции выполняются для высокотоксичных веществ, утилизация которых другими способами экономически нецелесообразна, и для радиоактивных отходов, которые нельзя нейтрализовать физическими или химическими способами.

Утечка информации о радиоактивных веществах возможна в результате выноса радиоактивных веществ сотрудниками организации или регистрации злоумышленником их излучений с помощью соответствующих приборов, рассмотренных в разд. III. Утечка информации о радиоактивных веществах возможна по двум ка-

налам: оптическому, носителями информации в котором являются электромагнитные поля в виде γ-излучений, и вещественному, носителями информации в котором являются элементарные α- и β-частицы.

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для α-излучений она составляет в воздухе единицы мм, β-излучений — см, только γ-излучения можно регистрировать на удалении в сотни и более метров от источника излучения.

### 6.8.2. Методы добывания информации о вещественных признаках

Вещественные признаки продукции, содержащие защищаемую информацию, определяются в результате химического, физико-химического и физического анализа. Основу химического анализа составляют химические реакции изучаемого вещества в растворе. Физико-химический анализ предусматривает измерение физических величин, изменение которых обусловлено химическими реакциями. Физический анализ учитывает изменение физических характеристик добытой пробы, вызванных исследуемым веществом.

Принципы и методы определения химического состава вещества рассматривает аналитическая химия, которая включает **качественные** и **количественные методы анализа**. Для аналитической химии характерно применение не только традиционных химических методов, но и физико-химических и физических методов, а также биологических методов.

**Качественный анализ** представляет собой совокупность методов установления химического состава путем идентификации атомов, ионов, молекул, входящих в анализируемое вещество. Основными показателями качественного анализа являются **специфичность** и **чувствительность**. Специфичность характеризует возможность метода обнаруживать искомое вещество в присутствии других элементов. Чувствительность определяется наименьшим количеством вещества, которое может быть обнаружено рассматриваемым методом. Чувствительность современных методов качественного анализа составляет порядка 1 мкг.

**Количественный анализ** использует совокупность методов определения количественных соотношений, в которых находятся элементы или отдельные соединения в анализируемом веществе. Показатели количественного анализа — **специфичность, чувствительность и точность**. Чувствительность и точность измеряются в процентах содержания исследуемого вещества в пробе. Чувствительность современных методов достигает $10^{-12}$–$10^{-15}$%. Точность, выражаемая значением относительной ошибки, составляет 1–2%.

Основными методами аналитической химии являются:

- методы разделения веществ;
- термические методы;
- химические методы;
- электрохимические методы;
- хроматографические методы;
- спектральный анализ;
- масс-спектрографические методы;
- радиоактивные методы;
- биологические методы.

**Разделение** — операция, в результате которой отделяются один от другого компоненты, составляющие исходную смесь. Для разделения применяются такие процессы как:

- осаждение, основанное на различной растворимости соединений в водных растворах;
- экстракция — процесс распределения вещества между двумя фазами;
- сорбция — поглощение газов, паров или растворенных веществ твердыми или жидкими поглотителями — сербентами;
- электровыделение (электролиз), при котором отделяемое вещество выделяют на твердых электродах;
- электрофорез, основанный на различиях в скоростях движения частиц разного заряда, формы и размера в электрическом поле;
- цементация, заключающаяся в восстановлении компонентов на металлах с отрицательными потенциалами;
- простая отгонка (выпаривание) — удаление веществ, находящихся в форме готовых летучих соединений;

- возгонка (сублимация) — перевод вещества из твердого состояния в газообразное и последующее осаждение его в твердой форме, минуя жидкую фазу;
- кристаллизация — образование зародышей твердой фазы при охлаждении газа, расплава или раствора.

**Термические методы** анализа используют термические эффекты, которые являются причиной или следствием химических реакций, и процессы выделения или поглощения теплоты в результате физических процессов.

В основе **химических методов** анализа лежат химические реакции трех типов: кислотно-основные, окислительно-восстановительные и комплексообразования. Основными из них являются классические гравиметрический и титриметрический методы. Гравиметрический метод заключается в выделении (путем осаждения, отгонки и т. д.) в чистом виде вещества и его взвешивании. Титриметрический метод основан на измерении количества реагента, затрачиваемого на реакцию с определяемым веществом. Методы, основанные на учете скорости химической реакции в зависимости от концентрации взаимодействующих веществ, представляют собой кинетические химические методы.

**Электрохимические методы** анализа изучают и используют процессы, протекающие не поверхности электрода и в приэлектродном пространстве. Различают прямые и косвенные электрохимические методы. В прямых методах используют связь между силой тока (величиной потенциала и т. д.) и концентрацией определяемого вещества, в обратных — зависимость измеряемого электрического параметра от объема титрата (раствора с определенной концентрацией).

**Хроматография** — физико-химический метод разделения и анализа смесей, основанный на распределении их компонентов между подвижными и неподвижными веществами. Жидкость или газ (подвижное вещество) протекают мимо неподвижного твердого вещества или пленки жидкости, нанесенной на него. Хроматографические методы классифицируются по агрегатному состоянию смеси (газ, жидкость), по механизму разделения, по форме проведения хроматографического процесса (колоночная, капиллярная, плоскостная).

**Спектральный анализ** проводится с целью определения состава вещества по его спектру. Различают атомарный, молекулярный спектральный, эмиссионный (по спектрам излучения) и адсорбционный (по спектрам поглощения) методы анализа. В качественном анализе полученный спектр идентифицируют и интерпретируют с помощью таблиц и атласов спектров элементов и индивидуальных соединений. В количественном спектральном анализе определяют состав вещества по относительно или абсолютной интенсивностям полос спектра.

**Масс-спектрометрические методы** позволяют исследовать вещества путем определения масс и распределения частиц, содержащихся в веществе. С этой целью производится ионизация атомов и молекул изучаемого вещества и разделение образующихся ионов в пространстве или времени.

Методы анализа веществ, основанные **на радиоактивности**, разделяют на группы: радиоактивный анализ, радиоиндикаторные, основанные на поглощении и рассеянии радиоактивных излучений, и радиометрические. Наиболее распространен радиоактивный метод исследования радиоактивного излучения нуклидов под воздействием потока элементарных частиц.

**Биохимические методы** используют биологические компоненты (ферменты, антитела и др.).

Если количество добытого вещества очень мало (порядка 100 мкг), то применяют **микрохимический анализ**, при меньшем количестве (единицы и доли мкг) — методы **ультромикрохимического анализа**.

Простейшие методы качественного микрохимического анализа предусматривают получение в капле раствора на фарфоровой пластинке окрашенных продуктов реакции и выделение в капиллярных пробирках осадков, характерных для конкретного элемента. В качественном микрохимическом анализе наиболее универсальным методом является **капельный анализ**, для которого раствор и высокочувствительные реагенты берутся в количестве нескольких капель. Для обнаружения определенных ионов используют характерные цветные реакции, которые проводят на фильтровальной бумаге, часовом стекле, капельной пластинке, в микротигле. Полуколичественная капельная калориметрия выполняется пу-

тем сравнения интенсивности окраски пятен, полученных на фильтровальной бумаге, с окраской стандарта. Чувствительность этого метода составляет (0,01–0,1) мкг.

В количественном микроанализе используются **гравиметрические**, **титрометрические**, **фотометрические** методы. Титрометрические методы занимают ведущее положение как наиболее простые и высокоточные. Предпочтение отдается электрохимическим методам титрования, прежде всего кулометрическим. Кулометрия — совокупность электрохимических методов анализа, основанных на измерении количества электричества, расходуемого при выделении на электроде того или иного вещества.

Весьма малые количества вещества (порядка $10^{-6}$ г и менее) исследуются методами **ультрамикрохимического анализа**. Приемы подготовки к анализу весьма специфичны и индивидуальные для каждого образца. Операции ультрамикрохимического анализа выполняются в капиллярной посуде через лупу (когда объем не менее $10^{-3}$ мл) и с помощью микроскопа с микроманипулятором (при объеме менее $10^{-3}$ мл). При наблюдении в микроскоп выполняют:

- осаждение в микроконусе с последующим отделением осадка центрифугированием;
- электролиз на микроэлектродах из тонкой проволоки;
- титрование в капиллярных ячейках;
- определение в виде окрашенных соединений в капиллярных кюветах с помощью микроскопов-фотометров.

В ультрамикрохимическом анализе органических веществ наряду с титрированием и спектрофотометрией применяют методы газовой **хроматографии** и **газового анализа**. Образцы для ультрамикрохимического анализа взвешивают на ультрамикровесах с точностью $10^{-9}$–$10^{-8}$ г. Проблемы анализа малых образцов обеспечиваются также сочетанием методов ультрамикрохимического исследования и физических методов.

## Вопросы для самопроверки

1. Особенности утечки информации по сравнению с утечкой материальных объектов.
2. Чем отличается технический канал утечки информации от канала связи?
3. Классификация технических каналов утечки информации.
4. Состав простых и составных каналов утечки информации.
5. Основные показатели технических каналов утечки информации.
6. Почему длина технического канала утечки информации является важным его показателем?
7. Виды и основные характеристики источников сигналов технических каналов утечки информации.
8. Виды и основные характеристики среды распространения технических каналов утечки информации.
9. Виды и основные характеристики приемников технических каналов утечки информации.
10. С какой целью комплексно используют технические каналы утечки информации?
11. Параметры источников сигналов, среды распространения и приемников сигналов акустических каналов утечки информации.
12. Что учитывает громкость звука? Диапазон громкости звуков в дБ и громкости речи в помещении.
13. Что представляет собой явление реверберации и как оно оценивается?
14. Какие составные каналы используются для повышения дальности передачи речевой информации?
15. Основные параметры источников сигналов, среды распространения и приемников сигналов оптических каналов утечки информации.
16. Какими показателями оценивается метеорологическая дальность видимости?
17. Основные показатели оптических волокон как световодов оптических каналов утечки информации.
18. Виды радиоэлектронных каналов утечки информации.
19. Виды сред распространения сигналов в радиоэлектронных каналах утечки информации.

20. Особенности распространения радиоволн различных диапазонов.
21. Способы повышения дальности распространения ультракоротких волн.
22. Виды помех в радиоэлектронном канале утечки информации.
23. Источники информации вещественных каналов утечки информации.
24. Методы добывания информации с использованием вещественных каналов утечки информации.

# Глава 7. Методы добывания информации

## 7.1. Основные принципы разведки

Жизненная необходимость в информации для любых государственных или коммерческих организаций вынуждает их расходовать людские, материальные и финансовые ресурсы на ее постоянное добывание. Так как любую работу эффективнее выполняют профессионалы, то эти структуры создают специализированные органы, предназначенные для добывания информации. Такими органами являются органы разведки.

Добывание информации органами разведки основывается на следующих принципах:

- целеустремленность;
- активность;
- непрерывность;
- скрытность;
- комплексное использование сил и средств добывания информации.

**Целеустремленность** предусматривает определение задач и объектов разведки, ведение ее по единому плану и сосредоточение усилий органов разведки на выполнении основных задач.

**Активность** предполагает активные действия всех элементов системы разведки по добыванию информации, прежде всего по поиску оригинальных способов и путей решения задач применительно к конкретным условиям.

**Непрерывность** разведки подчеркивает постоянный характер добывания информации и независимость этих действий от времени года, суток, погоды, любых условий обстановки. При изменении обстановки в соответствии с принципом активности меняются способы и средства добывания.

**Скрытность** ведения разведки обеспечивается путем проведения мероприятий по подготовке и добыванию информации в тайне, в интересах как безопасности органов добывания, так и скрытия фактов утечки или изменения информации. Реализация этого принципа позволяет разведке повысить безопасность органа добывания и выиграть время для более эффективного применения добытой информации. О том, что конфиденциальная информация

стала достоянием конкурента, руководство фирмы узнает обычно по косвенным признакам:

- снижению доходов или усилению позиций конкурента в связи с «выбросом» им на рынок аналогичных товаров, но с лучшими потребительскими свойствами или по более низким ценам;
- появлению публикаций в периодической печати и патентов по результатам исследований, ведущихся в лабораториях фирмы;
- перераспределению традиционной клиентуры в пользу конкурента.

Скрытность достигается применением пассивных технических средств, маскировкой и камуфлированием аппаратуры, легендированием и засекречиванием мероприятий по добыванию информации.

Учитывая многообразие способов и форм отображения информации, ориентация на способы и средства ее добывания, эффективные в определенных условиях, далеко не всегда приводит к положительным результатам в других условиях. Поэтому эффективное добывание информации проводится путем **комплексного использования различных способов и средств добывания информации**. Кроме того, при комплексировании обеспечивается дублирование данных, что является основным направлением повышения достоверности получаемой информации.

Добывание информации на основе указанных принципов осуществляется постоянно легальными способами и при недостаточности полученной этими способами информации — путем проведения тайных операций.

Легальное добывание информации проводится путем изучения и обработки по интересующим разведку вопросам публикаций в средствах массовой информации, периодических научных и популярных журналах, трудах высших учебных заведений и научно-производственных организаций, правительственных изданиях, учебных пособиях и др. Ценную информацию можно получить из открытых правительственных источников и отчетов. Нужную информацию можно найти в материалах, имеющих непосредственное отношение к деятельности фирмы: в соглашении о лицензиях, статьях и докладах, годовых отчетах фирм, отчетах коммивояжеров, обзорах рынков и докладов инженеров-консультантов, внутренних печатных изданиях, телефонных справочниках, рекламной

литературе и проспектах. Этот перечень можно многократно продолжить. По оценке заместителя начальника разведки ВМС США Захариаса во время Второй мировой войны разведка ВМС США получала 95% информации из открытых источников.

Органы обработки информации зарубежной разведки ведущих стран выписывают практически всю открытую центральную и местную печатную продукцию других государств. Результаты анализа возможностей добывания информации из легальных источников свидетельствуют, во-первых, о росте таких источников и, во-вторых, о том, что по мере роста объема мало управляемых информационных потоков все большая часть информации, содержащая тайну, попадает в открытые источники.

Однако наиболее ценная информация добывается нелегальным путем, в результате проведения тайных мероприятий спецслужбами и органами коммерческой разведки. Нельзя сбором и анализом сколь угодно большого объема открытых данных определить формулу и технологию нового вещества, если они изложены в документе, хранящемся за семью печатями.

Достаточно условно разведку можно разделить на **агентурную** и **техническую**. Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия — в преобладании человеческого или технического факторов.

Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента-разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

Развитие технической разведки связано, прежде всего, с повышением ее технических возможностей, обеспечивающих:

- снижение риска физического задержания агента органами контрразведки или службы безопасности за счет дистанционного контакта его с источником информации;
- добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

## 7.2. Классификация технической разведки

Многообразие видов носителей информации породило множество видов технической разведки. Ее классифицируют по различным признакам (основаниям классификации). Наиболее широко применяются две классификации: по физической природе носителей информации и видам носителей технических средств добывания.

Техническая разведка (при классификации по физической природе носителя информации) состоит из следующих видов (рис. 7.1):

- оптическая разведка (носитель — электромагнитное поле в видимом и инфракрасном диапазонах);
- радиоэлектронная разведка (носитель — электромагнитное поле в радиодиапазоне или электрический ток);
- акустическая разведка (носитель — акустическая волна в газообразной, жидкой и твердых средах);
- химическая разведка (носитель — частицы вещества);
- радиационная разведка (носитель — излучения радиоактивных веществ);
- сейсмическая разведка (носитель — акустическая волна в земной поверхности);
- магнитометрическая разведка (носитель — магнитное поле).

В связи с бурным развитием вычислительной техники самостоятельное значение приобретают силы и средства, добывающие информацию из компьютеров и вычислительных сетей. Классификационный признак для этого сравнительно нового вида технической разведки — **компьютерной разведки**, иной, чем для указанных видов рассматриваемой классификационной схемы, а именно — способы добывания информации. Основным способом добывания информации этим видом является перехват сигналов в компьютерах и их сетях. Учитывая, что компьютеры становятся основным средством обработки и хранения информации, возможности ее непрерывно растут.


*Рис. 7.1.* Классификация технической разведки по носителям информации

В свою очередь оптическая, радиоэлектронная и акустическая разведка подразделяется на подвиды технической разведки.

Оптическая разведка включает:

- визуально-оптическую;
- фотографическую;
- инфракрасную;
- телевизионную;
- лазерную.

Приведенная последовательность видов оптической разведки соответствует этапам развития оптической разведки по мере технического прогресса в области средств оптического наблюдения. В **визуально-оптической** разведке человек добывает информацию с помощью визуальных приборов. **Фотографическая разведка** позволяет регистрировать изображение объекта наблюдения на фотопленке. Средства **инфракрасной разведки** преобразуют изображение в инфракрасном диапазоне в видимое, но одноцветное изображение, цвет которого соответствует свечению люминофора экрана. **Телевизионная разведка** обеспечивает не только добывание информации о движущихся объектах, но и передачу этой информа-

ции на большое расстояние. **Лазерная разведка** решает две группы задач: получение информации по результатам облучения объекта лазерным лучом (для подсветки, измерения дальности, дистанционного физического и химического анализа) и определения источников и характеристик лазерного излучения. Последние 3 вида, использующие электронную технику, образуют **оптико-электронную разведку**. Технический прогресс размазывает границу между фотографической и оптикоэлектронной разведкой. Наряду с традиционными пленочными фотоаппаратами интенсивно развивается цифровая фотография. Основу ее составляют светоэлектрические преобразователи, на выходе которого эквивалентные изображению сигналы оцифровываются и в цифровой форме запоминаются в устройствах полупроводниковой или магнитной памяти.

**Радиоэлектронная разведка** в зависимости от характера добываемой информации подразделяется на:

- радиоразведку;
- радиотехническую разведку;
- радиолокационную разведку;
- радиотепловую разведку;
- разведку ПЭМИН.

**Радиоразведка** добывает, в основном, семантическую информацию путем перехвата радиосигналов с конфиденциальной информацией, радиотехническая — информацию о параметрах (признаках) радиотехнических сигналов, радиолокационная — о видовых признаках радиолокационного изображения объекта на экране радиолокатора, радиотепловая — о признаках, проявляющихся через собственные электромагнитные излучения объектов в радиодиапазоне. Силы и средства, используемые для добывания информации из побочных электромагнитных излучений и наводок, образуют разведку ПЭМИН, которая отличается от радиоразведки более чувствительной аппаратурой.

**Акустическая разведка** в зависимости от среды распространения акустической волны делится акустическую (в воздухе), гидроакустическую (в воде) и виброакустическую (в твердой среде, в основном в строительных конструкциях и различных трубах).

**Химическая разведка** добывает информацию о составе, структуре и свойствах веществ путем взятия проб и анализа их макрочастиц.

**Радиационная разведка** предназначена для обнаружения, локализации, определения характеристик и измерения уровней излучений радиоактивных веществ.

**Магнитометрическая разведка** позволяет по изменению магнитного поля Земли обнаруживать объекты, например подводные лодки в погруженном состоянии.

**Сейсмическая разведка** обеспечивает добывание информации из акустических (сейсмических) волн, распространяющихся в земной коре. Корректно включить в этот вид как подвид в акустическую разведку, как показано на рис. 7.1 пунктирной стрелкой. Однако в документах и структурно сейсмическая разведка выделена в отдельный вид.

Учитывая, что возможности технической разведки в значительной степени зависят от носителей ее технических средств, техническая разведка классифицируется также по виду носителей средств добывания (рис. 7.2).


*Рис. 7.2.* Классификация технической разведки по видам носителей средств разведки

Если средство добывания установлено на поверхности земли, в здании, на наземном транспорте, то такая разведка относится к **наземной**. На летающем аппарате (самолете, вертолете, воздушном шаре и др.) размещаются средства **воздушной разведки**. Добывание информации с использованием космических аппаратов осуществляет **космическая разведка**. Наконец, с помощью технических средств разведки, установленных на речных и морских судах (кораблях), ведется **морская разведка**.

## 7.3. Технология добывания информации

Независимо от принадлежности органа разведки и решаемых им задач технология добывания информации в общем случае представляет процесс, который начинается с момента постановки задачи ее пользователями (военно-политическим руководством страны или отдельных ведомств, руководством фирмы) до момента предоставления пользователям информации, соответствующей поставленным задачам и требованиям. Технология добывания информации предусматривает следующие этапы:

- организация добывания;
- добывание данных и сведений;
- информационная работа.

Любая деятельность без организации представляет собой хаотичный процесс. Организация добывания информации включает:

- декомпозицию (структурирование) задач, поставленных пользователями информации;
- разработку замысла операции по добыванию информации;
- планирование;
- постановку задач исполнителям;
- нормативное и оперативное управление действиями исполнителей и режимами работы технических средств.

Поставленные в достаточно общем виде задачи на добывание необходимой информации нуждаются в конкретизации с учетом имеющихся априорных данных о возможных источниках информации, их нахождении, способах доступа и преградах, параметрах используемых технических средств добывания и т. д. В результате анализа задач и априорных данных разрабатывается замысел операции, в котором намечаются пути решения поставленных задач.

На результативность добывания информации влияют многочисленные мешающие и случайные факторы — противодействие контрразведки государства и службы безопасности организаций, недостаточность априорной информации об источниках добываемых сведений и данных, отказы аппаратуры, погодные условия, бдительность граждан и сотрудников организации и др. Эти факторы учитываются при планировании и постановке задач с указанием места и времени действий всех исполнителей и технических средств, участвующих в операции по добыванию информа-

ции. Постановка соответствующих плану задач исполнителям перед проведением разведывательной операции рассматривается как **нормативное управление**. Но неучтенные факторы и изменившиеся условия требуют внесения корректив в процесс управления. Такое управление называется **оперативным**. Организацией добывания информации занимаются органы планирования и управления.

**Сведения и данные** добываются соответствующими органами путем поиска источников информации и ее носителей, их обнаружения, установления разведывательного контакта с ними, получения данных и сведений. Сведения и данные представляют фрагменты информации и отличаются друг от друга тем, что данные снимаются непосредственно с носителя, а сведения — проанализированные данные.

**Поиск объектов разведки** (источников и носителей информации, источников сигналов) производится в пространстве и во времени, а для носителей в виде полей и электрического тока — также по частоте сигнала. Поиск завершается обнаружением объектов разведки и получением от них данных.

**Обнаружение** интересующих разведку объектов в процессе поиска производится по их демаскирующим признакам и заключается в процедуре выделения объекта на фоне других объектов. Основу процесса обнаружения составляет процедура **идентификации** — отождествление путем сравнения текущих признаковых структур, формируемых в процессе поиска, с эталонной признаковой структурой объекта разведки.

Эталонные признаковые структуры содержат достоверные (по оценке органов разведки) признаки объекта или сигнала, полученные от первоисточников, например из документа или по данным, добытым из разных источников. Например, фотография в паспорте является эталонным описанием лица конкретного человека. Его признаковая структура состоит из набора признаков лица, которые криминалисты используют для составления фотороботов. Эталоны по мере изменения признаков корректируются. Например, несколько раз в течение жизни человека заменяются фотографии в паспорте, которые представляют собой эталонные изображения владельца паспорта для идентификации его личности. Эталонные признаковые структуры об объектах окружающего мира человек хранит

в своей памяти. Он постоянно их формирует в процессе развития, обучения и работы. Когда человек рождается, у него отсутствуют эталонные признаковые структуры объектов окружающего мира. В процессе собственных наблюдений и опыта, полученных знаний у него постепенно и постоянно формируются эталонные признаковые структуры, которые со временем корректируются. Например, когда человек встречает через 20 лет одноклассника, внешний вид которого существенно изменился, то вначале он может и не узнать своего бывшего приятеля, так как наблюдаемые (текущие) признаки отличаются от эталонных двадцатилетней давности. После получения подтверждения о том, что текущие признаки действительно принадлежат его школьному приятелю, в памяти производится корректировка эталона и при следующей встрече сомнения не возникают.

Путем идентификации текущей признаковой структуры с эталонной человек или автомат обнаруживают объект, которому соответствует эталонная признаковая структура. Чем больше признаков совпадает, тем выше вероятность обнаружения объекта.

Если эталонная признаковая структура отсутствует или принадлежность их к объекту вызывает сомнение, то процессу поиска объекта разведки предшествует этап поиска его эталонных (достоверных) признаков. Эталонные признаковые структуры постоянно накапливаются и корректируются при получении достоверных признаков. Полнота и достоверность эталонных признаковых структур для всех объектов, интересующих разведку или любую другую структуру, например правоохранительные органы, определяют необходимое условие эффективного обнаружения объекта.

Добытые данные, как правило, разрозненные. Они преобразуются в сведения, отвечающие на поставленные задачи, в ходе **информационной работы**, выполняемую органами сбора и обработки информации.

Информационная или аналитическая работа включает следующие последовательно выполняемые процессы:

- сбор и накопление данных и сведений от органов добывания;
- видовую обработку;
- комплексную обработку.

Данные и сведения (в случае предварительной обработки данных в органе добывания) передаются в орган видовой обработки.

Если в добывании информации участвуют органы различных видов, например, оптической и радиоэлектронной разведки, то осуществляется комплексная обработка сведений, поступивших от органов видовой обработки. Необходимость видовой обработки обусловлена различиями языков признаков, добываемых органами различных видов. Данные от органов добывания поступают, как правило, на языке признаков — параметры сигналов, изображения объектов разведки, координаты источников излучений и т. д. В результате видовой обработки синтезируется информация на профессиональном языке. В результате этого сведения, используемые для комплексной обработки, представляются на одном профессиональном языке. После комплексной обработки итоговая информация представляется на языке ее потребителей.

В ходе видовой и комплексной обработки формируются первичные и вторичные сведения на основе методов синтеза информации и процедур идентификации и интерпретации данных и сведений.

Формирование первичных сведений производится путем сбора и накопления данных и «привязки» их к тематическому вопросу, по которому добывается информация. Для включения данных в первичные сведения необходимо, чтобы эти данные содержали информационный признак о принадлежности данных к информации по конкретному вопросу. Например, если поставлена задача добывания информации о новом автомобиле, то добытые признаки его внешнего вида могут быть отнесены к этому автомобилю, если существует дополнительный признак (место, время или наличие возле него определенных лиц), которые с высокой степенью достоверности указывают на принадлежность признаков этому автомобилю. Если такой признак отсутствует, то имеет место простое **накопление данных**.

Формально при наличии в добытых данных Ах, Вх и Сх общего признака х, характеризующего принадлежность их к одному и тому же тематическому вопросу или объекту разведки, данные объединяются в первичные сведения АВСх. Любые новые данные, полученные от органа добывания, «привязывают», если это возможно, по общему признаку к первичным сведениям соответствующего объекта. В результате этого по мере добывания новых данных об объекте разведки его признаковая структура пополня-

ется новыми признаками, что приводит к увеличению различия ее по отношению к признаковым структурам других объектов.

Если полученные сведения отвечают на поставленные перед разведкой вопросы, то содержащаяся в сведениях семантическая и признаковая информация в соответствующей форме передается ее потребителям.

Необходимость в формировании вторичных сведений возникает тогда, когда не совпадают языки итоговой информации и первичных сведений, получаемых от органов добывания. Если потребителя интересуют видовые свойства продукции, создаваемой конкурентом, то добытые признаки внешнего вида не нуждаются в дополнительной обработке. Но когда для потребителя важны способы работы разрабатываемого технического средства, то первичные признаки не отвечают на эти вопросы. В этом случае формируются вторичные сведения не в виде, например, признаков внешнего вида или признаков сигналов, а в виде описания конструкции узлов и деталей новой продукции и принципов их работы, которые не удается добыть в виде оригиналов или копий.

Специалисты по внешнему виду могут по видовым признакам выявить особенности конструкции и работы продукции. Эти особенности не содержатся в первичных сведениях, у них даже разные языки. При формировании вторичных сведений возникает новая информация как результат **интерпретации** (толкования) первичных сведений. Основу интерпретации также составляет процесс сравнения текущей признаковой структуры объекта или его действий с эталонной. Только в отличие от идентификации в качестве эталонов используются причинно-следственные связи (продукции) между признаками типа «если, то». Например, если прибор содержит новый узел определенной конструкции, то характеристики прибора могут измениться таким-то образом. Язык продукции используется для создания экспертных систем с целью повышения эффективности принятия решений в различных областях деятельности, прежде всего в медицинской и технической диагностике. Процессы сбора и обработки вторичных сведений аналогичны соответствующим процессам для первичных сведений.

Видовая и комплексная обработка, в свою очередь, состоит из трех последовательно выполняемых процессов: осмысливание

данных и сведений, построение гипотезы, умозаключений и формулирование выводов, а также проверка выводов. Последняя операция выполняется с целью исключения грубых ошибок и пропуска дезинформации.

При формировании сведений применяются следующие методы синтеза информации:

- логические;
- структурные;
- статистические.

**Логические** методы используют для синтеза информации законы логики, учитывающие причинно-следственные связи в реальном мире. Они лежат в основе так называемого «здравого смысла» человека и являются основным методом синтеза информации человеком. Чем большими знаниями и опытом владеет человек, тем больше информативных связей он учитывает при принятии решения. Однако эти связи имеют и обратную сторону. Они консервируют логику мышления человека и тормозят процесс генерирования им новой информации ограничениями типа «этого не может быть». Люди, обладающие бурной фантазией, но лишенные консерватизма специальных знаний и опыта, — писатели-фантасты создают в своих произведениях модели будущих образцов техники, на десятилетия опережающие время их создания. В то же время прогнозы специалистов часто похожи на прототипы.

Причинно-следственные временные связи обеспечивают также выявление и прогнозирование действий объектов по признакам их деятельности в различные моменты времени.

**Структурные** методы учитывают объективно существующие связи между элементами объекта. Например, любой прибор имеет многоуровневую иерархическую структуру. Она включает блоки, узлы и детали, которые во время работы взаимодействуют друг с другом. Эти связи определяют конструкцию прибора и зафиксированы в конструкторской документации. При ее отсутствии специалисты восстанавливают конструкцию, назначение и функции по отдельным элементам и связям.

**Статистические** методы обеспечивают идентификацию и интерпретацию объектов и характера их деятельности по часто проявляющимся признакам, получаемым в результате статистической

обработки добываемых данных. В качестве таких признаков выступают статистически устойчивые параметры случайных событий: средние значения, дисперсии, функции распределения. Например, частое появление возле территории фирмы одних и тех же людей или автомобилей, обнаружение в помещениях фирмы закладных устройств служат признаками повышенного интереса конкурента или других субъектов к фирме или отдельным ее сотрудникам.

Таким образом, информационная работа включает аналитическую обработку больших массивов данных и сведений. Органы обработки широко привлекают к информационной работе в качестве аналитиков высококвалифицированных специалистов, которые интерпретируют данные и сведения. Кроме того, проводятся интенсивные работы по автоматизации процессов информационной работы.

## 7.4. Способы доступа органов добывания к источникам информации

Возможности разведки по добыванию информации зависят, прежде всего, от способов доступа ее органов добывания (агентов, технических средств) к источникам информации и обеспечения разведывательного контакта с ними. Эти факторы связаны между собой. Чем ближе удается приблизиться органу добывания к источнику информации, тем выше вероятность установления разведывательного контакта с ним.

Доступ к информации обеспечивается, когда источник (или носитель информации) обнаружен и локализован и с ним потенциально возможен **разведывательный контакт**. Установление разведывательного контакта между злоумышленником или его техническим средством и источником информации предусматривает выполнение условий, при которых злоумышленник непосредственно или дистанционно может похитить, уничтожить или изменить информацию. Условия разведывательного контакта — пространственное, энергетическое и временное.

**Пространственное условие** предполагает, что злоумышленник знает о месте нахождения источника информации или видит объект наблюдения. Если оно не известно, то источник приходится искать. Если область поиска велика, то процесс обнаружения ис-

точника информации может существенно затрудниться и затянуться во времени.

Так как любое перемещение носителя в пространстве уменьшает его энергию, то **энергетическое условие** разведывательного контакта состоит в обеспечении на входе приемника злоумышленника отношения сигнал/помеха, достаточного для получения на его выходе информации с требуемым качеством. Энергетическое условие учитывает не только энергию или мощность носителя, но и уровни различного рода мешающих воздействий (помех) одинаковой с носителем информации физической природы.

Помехи присутствуют в любой среде распространения, в любых средствах приема и обработки сигналов. Они могут при недостаточной мощности носителя вызвать такие искажения информации, при которых она станет непонятной получателю или у него возникнут сомнения в достоверности, особенно цифровых данных, которые наиболее легко подвергаются трансформации под действием помех. Поэтому получатель информации (санкционированный или нет) предъявляет такие требования к качеству информации, при выполнении которых у него не возникают сомнения в достоверности получаемой информации. Качество получаемой информации оценивается относительным количеством правильно принятых или искаженных элементов сообщения (букв, цифр, звуков речи, элементов изображения) или значениями искажений признаков объектов.

Так как добывание информации является динамичным процессом, то необходима синхронизация работы всех элементов, обеспечивающих этот процесс. Необходимость функционирования времени органа добывания, синхронизированного с временем возможности доступа к информации, составляет суть **временного условия** разведывательного контакта. При невыполнении его информацию не удастся получить даже в случае достаточной энергетики носителя. Действительно, если в кабинете ценного источника информации, например руководителя фирмы, установлено закладное устройство, которое позволяет прослушивать все ведущиеся в нем разговоры, а кабинет пуст, то временное условие не выполнено. Злоумышленник, находящийся в припаркованной вблизи территории фирмы машине, напрасно теряет время. Аналогичный результат наблюдается, когда в этом кабинете проводится совещание, но

приемник злоумышленника неисправен или изменилась нестабилизированная частота закладного устройства и «вышла» из полосы приемника злоумышленника, в результате чего приемник не принимает сигналы закладки и не выполняется пространственное условие в частотной области.

Таким образом, для добывания информации необходимы: доступ органа разведки к источнику информации и выполнение условий разведывательного контакта. Способы его несанкционированного доступа к информации можно разделить на три группы:

- физическое проникновение злоумышленника к источнику информации;
- сотрудничество злоумышленника с работником (гражданином другого государства или фирмы), имеющим легальный или нелегальный доступ к интересующей разведку информации;
- дистанционное добывание информации без нарушения границ контролируемой зоны.

Физическое проникновение к источнику информации возможно путем скрытого или с применением силы проникновения злоумышленника к месту хранения источника , а также в результате внедрения злоумышленника в организацию. Способ проникновения зависит от вида информации и способов ее использования.

**Скрытое проникновение** имеет ряд преимуществ по сравнению с остальными, но требует тщательной подготовки и априорной информации о месте нахождения источника, системе безопасности, возможных маршрутах движения и других сведений. Кроме того, скрытое проникновение не может носить регулярный характер, так как оно связано с большим риском для злоумышленника и приемлемо для добывания чрезвычайно ценной информации.

Для обеспечения **регулярного доступа к информации** проводится внедрение и легализация злоумышленника путем поступления его на работу в интересующую организацию. Так как при найме на работу претендент проверяется, то злоумышленник должен иметь убедительную легенду своей прошлой деятельности и соответствующие документы.

Рассмотренные способы обеспечивают скрытность добывания информации. Когда в ней нет необходимости, а цена информации очень велика, то возможно **нападение на сотрудников охра-**

**ны с целью хищения источника информации**. К таким источникам относятся, например, документы, которыми можно шантажировать конкурента или вытеснить его с рынка после публикации.

Для регулярного добывания информации органы разведки стараются привлечь к работе сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

Основными способами привлечения таких сотрудников являются следующие:

- инициативное сотрудничество;
- подкуп;
- сотрудничество под угрозой.

**Инициативное сотрудничество** предполагает привлечение людей, которые ищут контакты с разведкой зарубежного государства или конкурента, к сотрудничеству с целью добывания секретной или конфиденциальной информации по месту работы. Таких людей выявляют органы разведки путем наблюдения за сотрудниками и изучения их поведения, интересов, моральных качеств, слабостей, связей, финансового положения. В основе инициативного сотрудничества или предательства в подавляющем большинстве случаев лежат корыстные и аморальные мотивы, которые часто прикрываются рассуждениями о высоких целях.

Способы склонения к сотрудничеству подбираются под конкретного человека, который попал в поле зрения органов разведки и которого предполагается заставить сотрудничать (завербовать). Наиболее распространенным и менее опасным для злоумышленника способом склонения к сотрудничеству является **подкуп**. Подкупленный человек может стать постоянным и инициативным источником информации.

Другие способы склонения к сотрудничеству связаны с **насильственными действиями** злоумышленников. Это — психическое воздействие, угрозы личной безопасности, безопасности родных, имущества, а также преследования и шантаж, принуждающие сотрудника фирмы нарушить свои обязательства о неразглашении тайны. Если в результате предварительного изучения личностных качеств сотрудника фирмы, его жизни и поведения выявляются компрометирующие данные, то возможен шантаж сотрудника с целью склонения его к сотрудничеству под угрозой разгла-

шения компрометирующих сведений. Зарубежными спецслужбами иногда создаются для приезжающих в их страну специалистов различного рода провокационные ситуации с целью получения компрометирующих материалов для последующего шантажа.

**Выпытывание** — способ получения информации от человека путем задавания ему вопросов. Способы выпытывания разнообразны: от скрытого выпытывания до выпытывания под пыткой. Скрытое выпытывание возможно путем задавания в ходе беседы на конференции, презентации и или любом другом месте вроде бы невинных вопросов, ответы на которые для специалиста содержат конфиденциальную информацию.

Применяется скрытое выпытывание в устной или письменной форме при фиктивном найме сотрудника конкурирующей фирмы на более высокооплачиваемую или интересную работу. Причем приглашение доводится до сотрудника в форме, не вызывающей подозрение: через знакомых, в объявлении в средствах массовой информации об имеющейся вакансии по специальности сотрудника, но с существенно более высокой заработной платой и т. д. После получения в беседе с претендентом нужной информации ему под различными предлогами отказывают в приеме на работу.

Выпытывание под пыткой характерно для криминальных элементов, которые не утруждают себя применением скрытых, требующих длительной подготовки, способов добывания информации.

Добывание информации технической разведкой осуществляется в результате разведывательного контакта технических средств добывания с носителем информации, который распространяется в пространстве от ее источника. Если носитель информации распространяется за пределы контролируемой зоны, то возможно добывание информации без нарушения границ контролируемой зоны. Границей контролируемой зоны государства является государственная граница, границей контролируемой зоны организации — граница ее территории, которая отображается в общем случае забором. При распространении в пространстве носитель информации теряет энергию и все в большей степени изменяются под действием помех его информационные параметры, содержащие защищаемую информацию. Поэтому добывание информации возможно на таком удалении от источника, при котором обеспечивается до-

пустимое для злоумышленника качество получаемой информации, т. е. выполняется энергетическое условие разведывательного контакта. Чем дальше находится злоумышленник или его техническое средство от контролируемой зоны, тем меньше риск злоумышленника. Поэтому в общем случае контакт их с носителем осуществляется в зоне добывания, в которой качество добываемой информации не ниже допустимой, а риск минимален.

Способы доступа средств технической разведки к носителям без нарушения контролируемой зоны, т. е. с минимальным риском для злоумышленника, предусматривают размещение технических средств в местах вне контролируемых зон с выполнением энергетического условия разведывательного контакта. Кроме расстояния от источника на риск влияет скрытность добывания. Если добывание информации происходит за пределами контролируемой зоны организации, но действия злоумышленника(ов) вызывают подозрение у окружающих, то риск возрастает. Например, на фотографирующего здания и людей организации человека могут обратить внимание ее сотрудники, сообщить об этом службе безопасности, которая в зависимости от принадлежности организации может принять меры вплоть до привлечения правоохранительных органов и специальных служб к выяснению личности фотографа. Во всяком случае сам факт проявления интереса к организации повышает бдительность службы безопасности и активизирует ее работу по защите информации.

В общем случае за пределы контролируемой организации защищаемая информация переносится всеми носителями. Поэтому добывание информации без нарушения контролируемой зоны непосредственно или с помощью технических средств возможно путем подслушивания, скрытного наблюдения, перехвата сигналов с информацией, взятия проб воздуха, воды, твердых частиц возле территории организации. Если защищаемый источник находится на достаточно большом удалении от забора, то с целью обеспечения энергетического условия разведывательного контакта на территории организации или на ее границе скрытно устанавливают ретрансляторы — закладные устройства.

Добывание информации зарубежной технической разведкой без нарушения государственной границы возможно, учиты-

вая большие расстояния от источников сигналов до границы, для носителей с достаточно высокой энергией или малым затуханием в среде распространения. Такими носителями являются электромагнитные волны в оптическом и радиодиапазонах. Так как в каналах связи используются в основном высокочастотные сигналы, распространяющиеся в пределах прямой видимости, то дальность добывания информации зависит не только от мощности носителя информации и чувствительности приемника, но и высоты размещения средства разведки над земной поверхностью. Комплексы радио- и радиотехнической разведки размещаются на естественных высотах (холмах и горах) вблизи государственной границы. С развитием космической связи, каналы которой используются для обеспечения служебной связи и по которым передается закрытая информация, обеспечивается перехват радиосигналов средствами наземной разведки.

Наряду с наземными и надводными комплексами радио- и радиотехнической разведки широко применяют средства оптической и радиоэлектронной разведки, размещаемые на воздушных и космических аппаратах. В качестве воздушных аппаратов используются пилотируемые и беспилотные самолеты, а также привязные аэростаты. Самолеты барражируют на определенном участке вдоль государственной границы, а аэростаты крепятся в заданных местах с внутренней стороны границы с помощью троса. На платформе аэростата устанавливается малогабаритная приемная аппаратура, сигналы и электрический ток питания средств на платформе передаются по проводам троса.

Но максимальная высота подъема воздушных аппаратов, создающих подъемную силу за счет воздуха, составляет около 30000 м. В мирное время воздушная разведка источников и территории страны с эффективной ракетной противовоздушной обороны ведется без нарушения государственной границы. Максимальная дальность прямой видимости с высоты 30 км наземных объектов составляет около 600 км. Очевидно, что государство стремится удалить свои информативные источники информации, содержащей государственную тайну, подальше от границы.

Существенно большие потенциальные возможности доступа к объектам разведки имеет космическая разведка. Она позволяет

приблизить техническое средство добывания информации к любому объекту разведки на территории государства на расстояние 130–150 км и передать добытую информацию (изображения объектов, перехваченные сообщения) через спутники-ретрансляторы в реальном масштабе времени. Однако космическая разведка по сравнению с другими имеет ряд особенностей, существенно ограничивающих ее возможности:

1. Космические аппараты (КА) на низких круговых орбитах имеют высокую скорость движения относительно поверхности Земли (период вращения составляет около 90 минут), в результате чего время видимости объекта с КА составляет до 10 минут. За это короткое время можно получить фотографии объектов разведки, но оно недостаточно для ведения непрерывной радио- и радиотехнической разведки. С повышением высоты полета КА период его вращения увеличивается вплоть до 24 часов для геостационарных орбит. Но одновременно снижается энергия сигнала, достигающего средства КА.

2. Параметры орбит определяются с высокой точностью, что позволяет рассчитывать время пролета КА над любым защищаемым объектом и обеспечить его временное скрытие.

## 7.5. Показатели эффективности добывания информации

Наиболее общим показателем эффективности разведки, включающей органы управления, добывания и обработки, является степень выполнения поставленных перед нею задач. Для более объективного определения эффективности используется группа общесистемных показателей количества и качества информации, таких как:

- полнота добываемой информации;
- своевременность добывания информации;
- достоверность информации;
- вероятность обнаружения и распознавания объекта;
- точность измерения демаскирующих признаков;
- затраты на добывание информации.

**Полноту полученной информации** можно оценить отношением числа положительных ответов на тематические вопросы к

их общему количеству. Тематический вопрос определяет границы информации, необходимой для ответа на этот вопрос. Очевидно, что тематические вопросы можно детализировать до ответов на них в виде «да-нет»». Чем выше степень детализации тематических вопросов, тем точнее оценка полноты полученной информации. Тематические вопросы имеют иерархическую структуру и определяются в результате структурирования конфиденциальной информации при планировании мероприятий по ее добыванию. Поскольку тематические вопросы имеют различную значимость («вес»), то количественно полноту информации $П_и$ с учетом «веса» тематического вопроса можно приближенно оценить по формуле:

$$П_и = \sum_{i=1}^{n} \alpha_i \beta_i, \quad \sum_{i=1}^{n} \alpha_i = 1,$$

где $\alpha_i$ — «вес» i-го тематического вопроса; $\beta_i = 1$, когда количество и качество информации соответствуют i-му тематическому вопросу, и равно 0, когда не соответствует.

**Своевременность информации** является важным показателем ее качества, так как она влияет на цену информации. Если добытая информация устарела, то затраты на ее добывание оказались напрасными — она не может быть эффективно использована злоумышленником. Поэтому своевременность следует оценивать относительно продолжительности ее жизненного цикла. Если время устаревания информации существенно больше времени ее использования после добывания, то она своевременная. В противном случае она устаревшая.

**Достоверность информации** — важнейший показатель качества информации. Она искажается в результате дезинформирования и под действием помех. Так как использование ложной (искаженной) информации может нанести в общем случае больший ущерб, чем ее отсутствие, то выявлению достоверности добытой информации ее пользователь уделяет большое внимание.

Для оценки достоверности используют следующие частные показатели:

- достоверность сообщения в смысле отсутствия ложных сведения и данных;
- разборчивость речи;

- вероятность ошибочного или неискаженного приема дискретной единицы (бита, символа, цифры, буквы, слова).

Для количественной оценки достоверности сообщения могут применяться различные качественно-количественные способы и шкалы, в том числе так называемая схема Кента. В соответствии с ней диапазон возможных изменений достоверности разбивается на 7 интервалов и достоверность конкретной информации оценивается в шансах:

- достоверная информация (вероятность отсутствия ложной информации близка к 1);
- почти определено, что информация достоверна (9 шансов против одного);
- имеется много шансов, что информация достоверна (3 шанса против одного);
- шансы примерно равны (1 за, 1 против);
- имеется много шансов, что информация недостоверна (3 шанса против одного);
- почти определено, что информация недостоверна (за 9 шансов против одного);
- недостоверная информация (вероятность ложной информации близка к 1).

Достоверность информации в смысле отсутствия в ней элементов дезинформации зависит от надежности источника, которая может оцениваться по качественной шкале с уровнями:

- совершенно надежный;
- обычно надежный;
- довольно надежный;
- не всегда надежный;
- ненадежный;
- надежность не может быть определена.

Количество уровней не принципиально. Семь уровней выбрано как компромисс между точностью измерения (чем больше уровней, тем точность выше) и способностью эксперта интегрально оценивать достоверность информации. Известно, что человек в среднем способен одновременно оперировать с семью цифрами.

Качество подслушиваемой речи наиболее объективно оценивается показателем, называемым **разборчивостью речи**. В соответс-

твии с лингвистическим делением речи на фразы, слова, слоги и звуки разборчивость делят на **смысловую, слоговую и звуковую (формантную) разборчивость речи**. С точки зрения защиты речевой семантической информации наиболее наглядным является показатель смысловой разборчивости (разборчивости фраз). Однако получение объективных оценок смысловой разборчивости затруднено из-за избыточности речи. Более надежные результаты получаются при определении слоговой или звуковой разборчивости. Поэтому они получили наибольшее распространение.

**Разборчивость речи соответствует выраженной в процентах доли принятых без искажения единиц (фраз, слов, букв, звуков) по отношению к общему количеству переданных**. Избыточность письменной или устной речи снижает требования к значениям разборчивости и обусловлена различными значениями частоты использования в речи букв, а также существенно меньшим количеством разрешенных грамматикой слогов, слов и фраз по отношению к возможным комбинациям слогов, слов и фраз, которые теоретически можно составить из букв алфавита. Достаточно сказать, что в течение 80% времени телефонного разговора абоненты обмениваются лишь 155 разными словами.

В национальных языках следующие друг за другом слова связаны между собой смыслом и синтаксисом грамматики, а последовательно расположенные буквы в пределах одного слова — правилами орфографии. Чем больше букв в алфавите, меньше словарный состав языка и строже правила грамматики, тем выше избыточность языка. Неопределенность (энтропия) появления буквы русского алфавита из 32 букв при равновероятном выборе равна $H_0 = \log 32 = 5$ бит, с учетом реальной статистики одной буквы $H_1 = 4{,}35$ бит, двух букв подряд $H_2 = 3{,}52$ бит, трех — 3,01 бит. Для латинских языков энтропия букв принимает меньшие значения: $H_0 = 4{,}76$ бит, $H_1 = 4{,}03$ бит (английский язык), $H_1 = 4{,}1$ бит (немецкий язык), $H_1 = 3{,}96$ бит (французский язык). При увеличении количества учитываемых букв энтропия стремится к предельной величине $H_{пр}$. Разность $R = 1 - H_{пр}/H_0$ названа К. Шенноном **избыточностью языка**. Она характеризует долю (в процентах) неиспользуемых элементов языка из потенциально возможных.

В зависимости от количества учитываемых букв и анализируемых текстов различными авторами получены отличающиеся

оценки разборчивости. Избыточность разговорной речи в силу ее большей «вольности», меньшей стесненности правилами стилистики и даже грамматики меньше избыточности деловых текстов (табл. 7.1) [18].

*Таблица 7.1*

| *Форма представления* | *Избыточность, %* | |
|---|---|---|
| | *русского языка* | *французского языка* |
| Язык в целом | 72,6 | 70,6 |
| Разговорная речь | 72,0 | 68, |
| Литературные тексты | 76,2 | 71,0 |
| Деловые тексты | 83,4 | 74,4 |

Соотношения между качеством речи и количественными значениями слоговой и словесной разборчивости приведены в табл. 7.2 [19].

*Таблица 7.2*

| *Понятность речи* | *Разборчивость,%* | |
|---|---|---|
| | *слоговая* | *словесная* |
| Предельно допустимая | 25–40 | 75–87 |
| Удовлетворительная | 40–56 | 87–93 |
| Хорошая | 56–80 | 93–98 |
| Отличная | 80–100 | 98–100 |

Искажение слогов оказывает существенно меньшее влияние на понимание смысла семантической информации, заключенной в предложении или фразе, чем искажение целого слова. За счет словесной избыточности слово может быть восстановлено при отсутствии части букв или слога, что наглядно иллюстрируется в игре «Поле чудес»». Поэтому, требования к словесной разборчивости, что видно из табл. 7.2, более жесткие, чем к слоговой. Предельное минимальное значение разборчивости слогов и слов, при которых невозможно понять смысл речевого сообщения, равно 25 и 75% соответственно.

Цифровые данные также обладают избыточностью, но в контексте конкретного сообщения. Например, если в газете в июле месяце появляется прогноз погоды в Москве о температуре 0 или

50 градусов, то читатель этому сообщению не поверит и предположит об ошибке при верстке газеты. Однако исправить, т. е. указать точные значения цифр, он не сможет. Поэтому к достоверности передачи цифровых данных предъявляются высокие требования по достоверности передачи: одна ошибка и менее на миллион цифр. В ответственных случаях для повышения достоверности цифры пишутся прописью, как, например, принято при оформлении финансовых документов. В этом случае существенно понижается вероятность искажения цифр как под воздействием помех при передаче по каналам связи, так и в результате преступных действий злоумышленников.

Математический аппарат для определения достоверности приема дискретных элементов достаточно хорошо разработан в теории связи. В ней получены аналитические выражения, позволяющие вычислять вероятность приема символа или слова в зависимости от метода модуляции сигнала, вида помехоустойчивого кода, от отношения сигнал/шум на входе приемника. Например, формула для оценки **вероятности ошибочного приема двоичной единицы (бита)** в условиях флуктуационной помехи — шума имеет вид:

$$P_{ош} \approx 0{,}5[1 - \Phi(kq)],$$

где q — отношение сигнал/шум по амплитуде;

$$\Phi(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp(-y^2)dy,\ x = kq,$$

$k = 1/\sqrt{2}$ — амплитудная модуляция; $k = 1$ — частотная модуляция; $k = \sqrt{2}$ — фазовая модуляция.

**Точность n измерений значений признака** x оценивается среднеквадратичным отклонением, равным величине:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x_c)^2}{n}},\ \text{где } X_c = \frac{\sum_{i=1}^{n} x_i}{n}.$$

Кроме показателей количества и качества информации на этапе поиска и обнаружения объектов для оценки возможностей средств добывания используют такие показатели как вероятность обнару-

жения объектов и их распознавания (определение по измеренным демаскирующим признакам принадлежности объекта, его назначения, функций и свойств).

**Вероятность обнаружения и распознавания объекта** определяется как мера идентификации текущей признаковой структуры, полученной при наблюдении объекта, с эталонной. Чем больше признаков текущей структуры совпадает с эталонными признаками объекта и чем больше их информативность, тем выше вероятность обнаружения объекта. При распознавании объектов используется тот же механизм. Для достаточно достоверной оценки величины угроз безопасности информации необходимо определение возможностей и путей попадания информации к злоумышленнику.

### Вопросы для самопроверки

1. Принципы разведки.
2. Классификация технической разведки по видам носителя информации и средств разведки. Чем отличается разведка ПЭМИН от радиоэлектронной разведки?
3. Основные этапы и процессы добывания информации.
4. Чем нормативное управление отличается от оперативного управления?
5. Чем видовая обработка данных и сведений отличается от комплексной обработки?
6. Методы синтеза информации.
7. Условия разведывательного контакта органа добывания с объектом разведки.
8. Способы доступа к информации без нарушения контролируемой зоны организации.
9. Способы доступа к информации без нарушения государственной границы.
10. Преимущества и недостатки космической разведки на низкоорбитальных космических аппаратах.
11. Показатели эффективности разведки.
12. Какими показателями оценивается качество подслушиваемой речи?

# Глава 8. Методы инженерно-технической защиты информации

Любой метод решения задач учитывает основные факторы (условия), влияющие на результат. Факторы влияния на инженерно-техническую защиту информации можно разделить в соответствии с видами угроз.

## 8.1. Факторы обеспечения защиты информации от угроз воздействия

Случайные и преднамеренные воздействия на источники информации, охраняемые системой инженерно-технической защиты информации, можно представить в виде модели, приведенной на рис. 8.1.

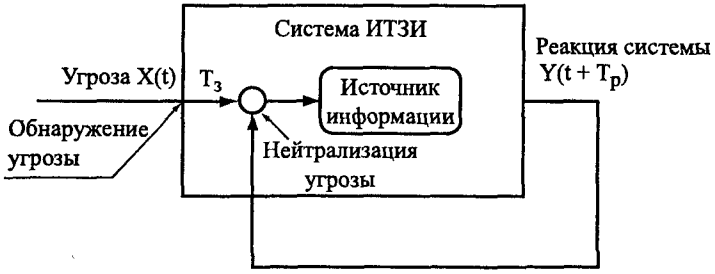



*Рис. 8.1.* Угрозы воздействия и реакция на них системы ИТЗИ

В текущий момент времени на вход системы ИТЗИ поступает k-я угроза воздействия, которая в случае обнаружения вызывает через время реакции системы $\tau_р$ меру по нейтрализации этой угрозы. Нейтрализация угрозы возможна только в том случае, если источник угрозы за время реакции не достигнет источника информации. В противном случае источник угрозы успеет воздействовать на источник информации, в результате чего изменится, будет уничтожена или похищена содержащаяся в нем информация. То же произойдет, если угроза не будет обнаружена. Возможен также вариант, когда возникнет ложный сигнал об угрозе при ее фактическом отсутствии. Очевидно, что на безопасности информации такой вариант на отразится, но увеличатся затраты на меры защиты, что снизит эффективность защиты.

Временные показатели системы ИТЗИ (время реакции и задержки) в общем случае величины случайные, так как они зависят от большого числа факторов. Если угрозу, например, создает злоумышленник, стремящийся проникнуть к месту хранения источника информации, то время его движения зависит от множества различных факторов. К ним относятся априорные знания злоумышленника о системе защиты (о количестве и прочности преград на пути его движения, средствах охраны и нейтрализации вторжений и др.), квалификация злоумышленника, возможности его технических средств, используемых им для преодоления этих преград, и т. д.

Время реакции системы определяется организацией охраны, удаленностью места проникновения злоумышленника от места размещения сил и средств нейтрализации угрозы, временем обнаружения злоумышленника на территории организации, скоростью движения их к месту нахождения злоумышленника и т. д. При достаточно большом числе независимых факторов распределение этого времени можно аппроксимировать нормальным законом.

Для обеспечения безопасности информации необходимо или уменьшать время реакции системы до значения, меньшего времени задержки злоумышленника, или укреплять преграды путем увеличения времени задержки до значения, большего времени реакции.

Так как время реакции людей зависит от их психологической установки на нейтрализацию угроз, то при повышении вероятности ложных тревог средств охраны время реакции может также увеличиться, а вероятность $P(\tau_р < \tau_з)$ — уменьшиться.

С учетом рассмотренных соображений вероятность $P_{ур}$ реализации угрозы воздействия определяется как:

$$P_{ур} = P_{нв} + P_{ов}P(\tau_р < \tau_з),$$

где $P_{ов}$ и $P_{нв}$ — вероятности обнаружения и необнаружения источника угрозы соответственно.

Суммарная вероятность воздействия источника угрозы информации на ее источник может быть оценена в соответствии с выражением:

$$P_{ув} = P_{ву}[P_{нв} + P_{ов}P(\tau_р < \tau_з)],$$

где $P_{ву}$ — вероятность возникновения угрозы воздействия.

Из анализа этого выражения следует, что для эффективной защиты информации необходимо:

- увеличивать вероятность обнаружения угрозы воздействия;
- уменьшать вероятность появления ложного сигнала об угрозе;
- уменьшать время реакции системы на угрозу с момента обнаружения ее источника;
- увеличивать время задержки источника угрозы.

## 8.2. Факторы обеспечения защиты информации от угроз утечки информации

Угрозы утечки информации возникают, когда создаются предпосылки несанкционированного распространения носителя информации от ее источника до злоумышленника. Процесс утечки можно разделить на два последовательных этапа: образование канала утечки и распространение по нему защищаемой информации. Так как в общем случае характеристики носителей опасных сигналов каналов утечки информации злоумышленнику неизвестны, то для снятия с них информации он должен обнаружить эти носители, установить с ними контакт и получить (снять) с них информацию. На эффективность защиты информации от утечки влияют следующие факторы:

- условия образования технического канала утечки информации;
- время и затраты на поиск носителя с защищаемой информацией;
- вероятность обнаружения и распознавания носителя информации;
- отношение сигнал/шум на входе приемника сигналов (контраст изображения, концентрация демаскирующего вещества в пробе), определяющее качество добываемой информации;
- вероятность распознавания объекта защиты по добываемым признакам.

Условия образования технических каналов утечки информации могут быть для злоумышленника случайными или им создаваемыми. Например, побочное высокочастотное излучение радиоэлектронного средства, размещенного в выделенном помещении, не зависит от злоумышленника. Поэтому частота излучения для злоумышленника не известна, и ему с целью использования этого

излучения для подслушивания придется ее искать. Если злоумышленник организует канал утечки информации, например, путем установки в помещении закладного устройства, то частота известна, но не известно время ведения закрытых переговоров.

Поиск носителя с информацией в зависимости от его вида может быть в пространстве и по частоте. Время и затраты на поиск носителя информации зависят от априорных данных о его месте расположения и частоте. Если эти данные отсутствуют, то поиск осуществляется путем сканирования части пространства и диапазона частот, в пределах которых может находиться носитель. Таким образом осуществляют сканирование воздушного пространства средства ПВО страны или частотного диапазона при поиске службой контроля эфира незарегистрированного передатчика. Очевидно, что временные и другие затраты зависят от объема пространства и диапазона частот, в которых производится поиск, а также характеристик средств поиска. Например, время поиска случайного опасного сигнала с речевой информацией, генерируемого побочным высокочастотным излучением в диапазоне от единиц МГц до единиц ГГц, может составлять часы. Поиск завершается обнаружением и распознаванием носителя.

Вероятность обнаружения объекта разведки определяется значением произведения безусловной вероятности обнаружения его признаков и условной (после обнаружения) вероятности идентификации объекта по обнаруженным признакам. Когда время проявления признаков меньше времени поиска объекта, то во время поиска объект может быть пропущен. Например, если во время настройки приемника злоумышленника на частоту побочного излучения из кабинета руководителя организации в нем отсутствует речевая информация, то злоумышленник принимает сигнал излучения как помеху и перестраивает радиоприемник. Вероятность обнаружения признаков объекта разведки $P_{оп}$ приблизительно можно оценить как отношение времени проявления признаков $\tau_{пп}$ к времени поиска $T_{по}$, т. е. $P_{оп} \approx \tau_{пп}/T_{по}$.

Обнаружение объекта по его признакам представляет собой процесс сравнения множества текущих признаковых структур с эталонной признаковой структурой объекта разведки (объекта наблюдения, сигнала, вещества), а распознавание — путем сравнения текущей признаковой структуры обнаруженного объекта с

множеством признаков, описывающих его характеристики — тип, назначение, структуру, параметры и др. (см. рис. 8.2.).

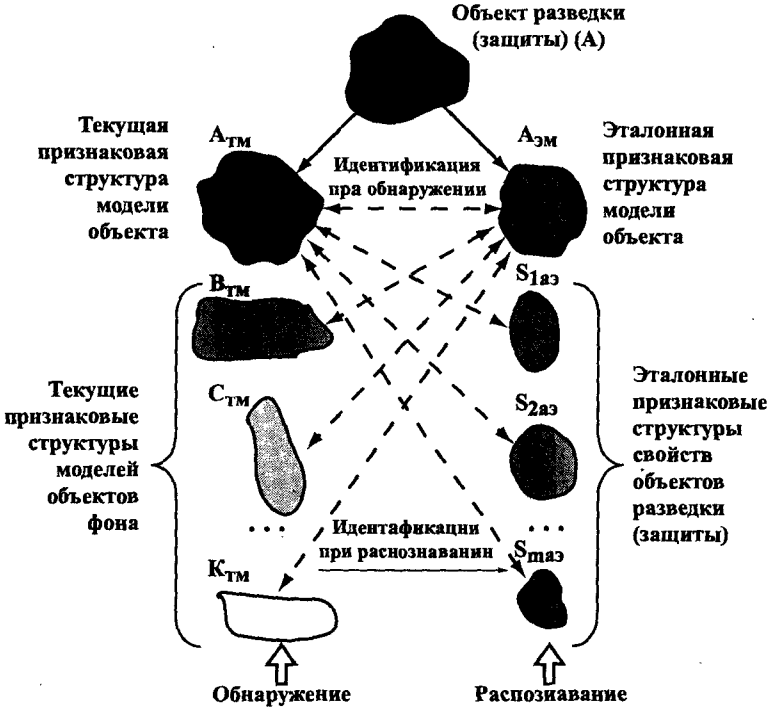



Рис. 8.2. Схема процедур обнаружения и распознавания объектов

Объект или его характеристики идентифицируются (отождествляются) по максимуму близости текущих и эталонных признаковых структур рассматриваемых объектов и их свойств. Основу процессов обнаружения и распознавания составляет процедура **идентификации признаковых структур**.

Идентификация представляет собой процедуру определения близости двух признаковых структур (текущей и эталонной) с учетом информативности их признаков. Представим информационную емкость текущей признаковой структуры через $S_{ит}$, а информационную емкость эталонной структуры через $S_{из}$. Графически близость двух структур можно представить в виде пересечения диаграмм Венна с общей областью $S_{итэ}$. Когда диаграммы Венна, соот-

ветствующие текущей и эталонной признаковым структурам пересекаются, то меру их близости (коэффициент идентичности) можно характеризовать как $К_{ин} = S_{итэ}/(S_{ит} + S_{иэ} - 2S_{итэ})$ (рис. 8.3). Если все признаки структур совпадают, то структуры идентичны по рассматриваемым признакам. Если все признаки одной структуры с меньшей информационной емкостью совпадают с признаками другой структуры, имеющей большую информационную емкость, то мера близости (коэффициент идентичности $К_{ин}$) оценивается отношением меньшей информационной емкости к большей.

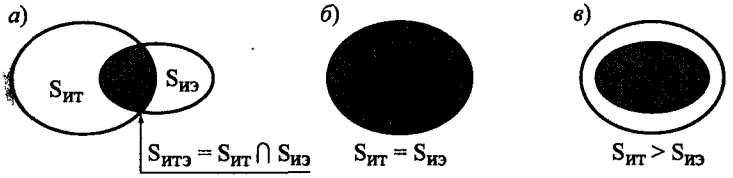



Рис. 8.3. Диаграммы Венна текущей и эталонной признаковых структур

Следовательно, вероятность идентификации структур зависит от количества и информативности общих для них демаскирующих признаков. Обозначим вероятность присутствия к-го признака в эталонной признаковой структуре через $Р_{эк}$, а через $Р_{тк}$ — вероятность обнаружения этого признака при формировании текущей признаковой структуры. Вероятность наличия к-го признака в обеих структурах равна произведению вероятностей $Р_{эк}Р_{тк}$.

Информативность к-го признака признаковой структуры зависит от ошибки $\Delta_к$ его измерения на модели объекта относительно значения этого признака у реального объекта. В первом приближении зависимость $I_к(\Delta_к)$ можно представить в виде $I_к(\Delta_к) = I_{ок}\exp(-\alpha_к\Delta_к)$, где $I_{ок}$ — информативность к-го признака объекта, $\alpha_к$ — коэффициент, учитывающий влияние точности измерения признака на его информативность. При нулевой ошибке измерения признака информативность признака признаковой структуры будет соответствовать информативности этого признака объекта. При увеличении ошибки измерения информативность признака стремится в пределе к нулевому значению. Так как на вероятность идентификации объекта влияет информативность к-го признака в эталонной и текущей признаковых структурах, то инфор-

мативность общего для этих структур к-го признака можно оценить величиной $I_{ок}\exp[-\alpha_к(\Delta_{эк} + \Delta_{тк})]$.

Следовательно, в общем случае вероятность идентификации объекта по к-му признаку можно представить в виде функции, зависящей от вероятности $P_{эк}$ включения к-го признака в эталонную признаковую структуру объекта, вероятности $P_{тк}$ его обнаружения и включения в текущую признаковую структуру, информативности этого признака с учетом точности его измерения при образовании эталонных и текущих признаковых структур:

$$Q_k = P_{эк}P_{тк}I_{ок}\exp[-\alpha_к(\Delta_{эк} + \Delta_{тк})].$$

Точность измерения признаков зависит от разрешающей способности средства добывания и соотношения мощности носителя в виде сигнала и мощности других носителей — помех. В теории связи определены зависимости вероятности обнаружения и распознавания сигналов от отношения сигнал/шум на входе приемника.

Вероятность идентификации объекта по m признакам эталонной и текущей структур оценивается в соответствии с выражением:

$$Q_и \le 1 - \prod_{k=1}^{m}(1 - Q_k),$$

где m — количество общих признаков для эталонной и текущей структур моделей объекта.

Знак $\le$ учитывает зависимость признаков. Максимальное значение вероятность идентификации принимает для независимых признаков; минимальное, равное вероятности идентификации по одному признаку при коэффициенте корреляции между признаками, равном 1. Управляя рассмотренными факторами, можно обеспечить требуемый уровень безопасности информации, при котором вероятность идентификации объекта органом разведки меньше нормативного значения.

После обнаружения и идентификации носителя с защищаемой информацией ее утечка возможна, если отношение мощности (амплитуды) носителя и мощности (амплитуды) помех на входе приемника злоумышленника превосходит определенное значение, зависящее от вида информации и ее носителя, метода записи инфор-

мации на носитель, требований к качеству добываемой информации и др. В явном виде это отношение определяется для акустических и радиосигналов. Для оптических сигналов эта величина соответствует абсолютному контрасту изображения объекта по отношению к изображению фона. В вещественном канале утечки информации, например, после получения пробы с демаскирующим веществом возможность определения вещественных признаков зависит от концентрации демаскирующего вещества в смеси пробы.

Так как добываемая информация содержится в признаках объекта, то возможность утечки информации зависит от вероятности распознавания этих признаков.

Таким образом, риск (вероятность) утечки информации по техническому каналу можно оценить в виде произведения вероятностей следующих событий:

- образования технического канала утечки информации;
- обнаружения в результате поиска носителя с информацией;
- требуемого превышения мощности носителя по отношению к мощности помех;
- распознавания объекта защиты (разведки).

Следовательно, для предотвращения утечки информации по техническому каналу необходимо:

- устранить условия, способствующие образованию технических каналов утечки информации;
- скрыть демаскирующие признаки носителя информации в каналах утечки;
- уменьшить мощность носителя в месте возможного размещения приемника злоумышленника;
- уменьшить информативность признаковой структуры объектов защиты.

## 8.3. Классификация методов инженерно-технической защиты информации

Как следует из факторов, влияющих на эффективность инженерно-технической защиты информации, ее методы должны обеспечить реализацию следующих направлений инженерно-технической защиты информации:


*Рис. 8.4.* Классификация направлений и методов инженерно-технической защиты информации

- предотвращение и нейтрализацию преднамеренных и случайных воздействий на источник информации;
- скрытие информации и ее носителей от органа разведки (злоумышленника) на всех этапах добывания информации.

Кроме того, учитывая, что для добывания информации злоумышленник может использовать различные специальные средства (закладные устройства, диктофоны и др.), третье направление включает методы обнаружения, локализации и уничтожения и этих средств, а также подавления их сигналов.

Первое направление объединяют методы, при реализации которых:

- затрудняется движение злоумышленника или распространение стихийных сил к источнику информации;
- обнаруживается вторжение злоумышленника или стихийных сил в контролируемую зону и их нейтрализация.

Классификация направлений и методов инженерно-технической защиты информации приведена на рис. 8.4.

Затруднение движения источников угроз воздействия к источникам информации обеспечивается в рамках направления, называемого **физической защитой**. Физическая защита обеспечивается методами инженерной защиты и технической охраны. Инженерная защита создается за счет использования **естественных** и **искусственных преград** на маршрутах возможного распространения источников угроз воздействия. Искусственные преграды создаются с помощью различных инженерных конструкций, основными из которых являются заборы, ворота, двери, стены, межэтажные перекрытия, окна, шкафы, ящики столов, сейфы, хранилища. Так как любые естественные и искусственные преграды могут быть преодолены, то для обеспечения надежной защиты информации, как и иных материальных ценностей, необходимы методы обнаружения вторжений в контролируемые зоны и их нейтрализации.

Эти методы называются **технической охраной объектов защиты**. Под объектами защиты понимаются как люди и материальные ценности, так и носители информации, локализованные в пространстве, К таким носителям относятся бумага, машинные носители, фото и кино пленка, продукция, материалы и т. д., то есть все, что имеет четкие размеры и вес. Носители информации в виде электромагнитных и акустических полей, электрического тока не

имеют четких границ и для защиты информации на этих носителях методы инженерной защиты не приемлемы — электромагнитное поле с информацией нельзя хранить, например, в сейфе. Для защиты информации на таких носителях применяют методы скрытия информации.

**Скрытие информации** (прятание, утаивание) объединяет группу методов защиты информации, основу которых составляют условия и действия, затрудняющие поиск и обнаружение объектов защиты, распознавание и измерение их признаков, снятие с носителей информации с качеством, достаточным для ее использования. Оно предусматривает такие изменения местоположения, времени передачи сообщения или проявления демаскирующих признаков, структуры информации, структуры и энергии носителей, при которых злоумышленник не может непосредственно или с помощью технических средств выделить информацию с качеством, достаточным для использования ее в собственных интересах. Скрывать от злоумышленника можно как информацию, так и ее носитель. Различают пространственное, временное, структурное и энергетическое скрытие.

**Пространственное скрытие** затрудняет поиск и обнаружение злоумышленником источника информации в пространстве. Оно достигается размещением источника информации в местах, местоположение которых априори злоумышленнику не известно. Такие места хранения называются **тайниками**. Перед злоумышленником возникает дополнительная задача — поиск источника. Чем больше область поиска, тем труднее найти объект. Подводные лодки представляют большую угрозу, прежде всего, потому, что обеспечивается их высокая пространственная скрытность. Возможные места для тайников рассмотрены в [20]. При создании тайников их авторы часто не учитывают шаблонность мышления большинства людей. Этим пользуются квартирные воры, которые легко находят места, в которых хозяева хранят свои ценности.

К пространственным можно отнести стеганографические способы защиты информации, которые предусматривают скрытное размещение защищаемой информации, отображаемой в символьной форме, в так называемых контейнерах. Контейнеры — свободные части носителя, содержащего другую информацию.

Наиболее древним стеганографическим способом скрытия информации является написание сообщения симпатическими (бесцветными без специальной тепловой или химической обработки) чернилами между строк письма или иного документа. Известно много способов записи данных, реализующих пространственное скрытие информации: запись наколом букв на оборотной стороне этикеток флаконов, банок или бутылок, на внутренней стороне спичечной коробки, внутри яйца и др. В годы расцвета фототехники для скрытной передачи сообщений использовалась так называемая «микроточка», изобретенная немецким ученым Э. Голдбергом. «Микроточка» представляла собой микроизображение разведывательного сообщения размером 0,01–1 мм$^2$, которое наклеивалось в качестве точки текста письма, открытки, под марку и иные места безобидной корреспонденции или предметов. Величина уменьшенных символов в «микроточке» достигала 1 микрона. Большие возможности по реализации стеганографических способов скрытия информации предоставляют компьютерные технологии записи информации. Компьютерная стеганография основывается на том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери качества изображения или звука. Такая возможность обусловлена неспособностью органов чувств человека различать незначительные изменения в цвете изображения или в частотах звука. Поэтому в качестве контейнеров используются графические и звуковые файлы, содержащие оцифрованное изображение и звук. Младшие (1–4) разряды используемых многоразрядных кодов могут быть изменены без ухудшения качества изображения или звука, в них можно записать секретную и конфиденциальную информацию и обеспечить ее эффективное скрытие. Например, качество эталонного изображения в формате bmp объемом 243 Кбайт незаметно отличается от того же изображения в файле которого помещена иная информация объемом 119 Кбайт.

Отсутствие у злоумышленника данных о времени передачи сообщения с интересующей информацией или времени проявления демаскирующих признаков объекта защиты вынуждает злоумышленника тратить большие ресурсы на обеспечение непрерывности разведки. Этим достигается **временное скрытие**. Десятки ты-

сяч операторов и технических средств Агентства национальной безопасности США постоянно и непрерывно «слушают» эфир в разных точках пространства в разных частотных диапазонах, чтобы не пропустить и перехватить информативное сообщение в каналах связи своего вероятного противника. Чем короче по времени передаваемое сообщение, тем сложнее его обнаружить. Поэтому одним из методов временного скрытия является передача с большой скоростью сообщения, накопленного за время, значительно превышающее время его передачи.

С другой стороны, если известно время возможной работы средств добывания, то существенно легче скрыть информацию. Хотя разведка ведется скрытно, но появление тех или иных носителей средств разведки (самолетов, кораблей, космических аппаратов, автомобилей с дипломатическими номерами) возле контролируемой зоны в большинстве случаев обнаруживается средствами соответствующих служб, что позволяет принять меры по скрытию информации. Например, «ахиллесовой пятой» наиболее эффективной в мирное время космической разведки является заблаговременное знание контрразведкой точного времени пролета низкоорбитального разведывательного космического аппарата. Службе безопасности порой достаточно для обеспечения эффективной защиты на короткое время (минуты) пролета прекращать информативные излучения и зачехлять защищаемые объекты, наблюдаемые сверху.

**Структурное скрытие** достигается изменением или созданием ложного информационного портрета семантического сообщения, физического объекта или сигнала.

**Информационным портретом** можно назвать совокупность элементов и связей между ними, отображающих смысл сообщения (речевого или данных), признаки объекта или сигнала. Элементами дискретного семантического сообщения, например, являются буквы, цифры или другие знаки, а связи между ними определяют их последовательность. Информационными портретами объектов наблюдения, сигналов и веществ являются их эталонные признаковые структуры.

Возможны следующие способы изменения информационного портрета [21]:

- удаление части элементов и связей, образующих информационный узел (наиболее информативную часть) портрета;
- изменение части элементов информационного портрета при сохранении неизменности связей между оставшимися элементами;
- удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Изменение информационного портрета объекта вызывает изменение изображения его внешнего вида (видовых демаскирующих признаков), характеристик излучаемых им полей или электрических сигналов (признаков сигналов), структуры и свойств веществ. Эти изменения направлены на сближение признаковых структур объекта и окружающего его фона, в результате чего снижается контрастность изображения объекта по отношению к фону и ухудшаются возможности его обнаружения и распознавания.

Но при изменении информационного портрета информация не воспринимается не только злоумышленником, но и ее санкционированным получателем. Следовательно, для санкционированного получателя информационный портрет должен быть восстановлен путем дополнительной передачи ему удаленных элементов и связей или алгоритма (ключа) этих изменений.

В условиях рынка, когда производитель вынужден рекламировать свой товар, наиболее целесообразным способом информационного скрытия является исключение из рекламы или открытых публикаций наиболее информативных сведений или признаков — информационных узлов, содержащих охраняемую тайну.

К **информационным узлам** относятся принципиально новые технические, технологические и изобразительные решения и другие достижения, которые составляют ноу-хау. Изъятие из технической документации информационных узлов не позволит конкуренту воспользоваться информацией, содержащейся в рекламе или публикациях.

Этот широко применяемый метод позволяет:

- существенно уменьшить объем защищаемой информации и тем самым упростить проблему защиты информации;
- использовать в рекламе новой продукции сведения о ней, не опасаясь разглашения.

Например, вместо защиты информации, содержащейся в сотнях и тысячах листов технической документации, разрабатываемой для производства новой продукции, защите подлежат всего несколько десятков листов с информационными узлами.

Структурное скрытие, в результате которого информационный портрет изменяется под информационный портрет фона, называется **маскировкой**. Методы маскировки отличаются для разных видов сообщения. Маскировка семантической информации, представляемой в виде набора определенным образом связанных символов, обеспечивается криптографическими методами и называется **шифрованием**. Фоном для маскируемого сообщения является случайный набор символов. Поэтому чем меньше зашифрованное сообщение отличается от случайного, тем выше уровень скрытия информации.

Маскировка признаковой информации достигается изменением информативных признаков объекта защиты под признаки объектов фона. В зависимости от вида признаковой информации маскируются признаки объектов наблюдения, сигналов или демаскирующих веществ. Фон при наблюдении образуют другие объекты, в том числе предметы местности. Фоном для сигналов являются другие сигналы — помехи. Но помехи в отличие от объектов фона при наблюдении могут изменять параметры сигналов, несущих защищаемую информацию. Если энергия помех выше энергии сигналов, то эти изменения столь значительны, что структура сигналов приближается к структуре помех. Следовательно, помехи маскируют сигнал. Так как степень воздействия помех и соответственно маскирующий эффект зависят от отношения мощности сигнала и помех, то метод маскировки сигнала помехами можно назвать энергетическим скрытием информационных сигналов.

**Энергетическое скрытие** достигается уменьшением отношения энергии (мощности) сигналов, т. е. носителей (электромагнитного или акустического полей и электрического тока) с информацией, и помех. Уменьшение отношения сигнал/помеха (слово «мощность», как правило, опускается) возможно двумя методами: снижением мощности сигнала или увеличением мощности помехи на входе приемника.

Воздействие помех приводит к изменению информационных параметров носителей: амплитуды, частоты, фазы. Если носите-

лем информации является амплитудно-модулированная электромагнитная волна, а в среде распространения канала присутствует помеха в виде электромагнитной волны, имеющая одинаковую с носителем частоту, но случайную амплитуду и фазу, то происходит интерференция этих волн. В результате этого значения информационного параметра (амплитуды суммарного сигнала) случайным образом изменяются и информация искажается. Чем меньше отношение мощностей, а следовательно, амплитуд, сигнала и помехи, тем значительнее значения амплитуды суммарного сигнала будут отличаться от исходных (устанавливаемых при модуляции) и тем больше будет искажаться информация.

Природные и промышленные помехи, которые постоянно присутствуют в среде распространения носителя информации, оказывают наибольшее влияние на амплитуду сигнала, в меньшей степени — на его частоту. Но ЧМ-сигналы имеют более широкий спектр частот. Поэтому в функциональных каналах, допускающих передачу более широкополосных сигналов, например, в УКВ-диапазоне, передачу информации осуществляют, как правило, ЧМ-сигналами как более помехоустойчивыми, а в узкополосных ДВ-, СВ- и КВ-диапазонах — АМ-сигналами.

В общем случае качество принимаемой информации ухудшается с уменьшением отношения сигнал/помеха. Характер зависимости качества принимаемой информации от отношения сигнал/помеха отличается для различных видов информации (аналоговой, дискретной), носителей и помех, способов записи на носитель (вида модуляции), параметров средств приема и обработки сигналов.

Наиболее жесткие требования к качеству информации предъявляются при передаче данных (межмашинном обмене): вероятность ошибки знака по плановым задачам, задачам статистического и бухгалтерского учета оценивается порядка $10^{-5}$–$10^{-6}$, по денежным данным — $10^{-8}$–$10^{-9}$. Для сравнения, в телефонных каналах хорошая слоговая разборчивость речи обеспечивается при 60–80%, т. е. требования к качеству принимаемой информации существенно менее жесткие. Это различие обусловлено избыточностью речи, которая позволяет при пропуске отдельных звуков и даже слогов восстанавливать речевое сообщение. Вероятность ошибки знака $10^{-5}$ достигается при его передаче двоичным АМ сигналом и отношении мощности сигнала к мощности флуктуационного шума на вхо-

де приемника приблизительно 20, при передаче ЧМ сигналом — около 10. Для обеспечения разборчивости речи порядка 85% превышение амплитуды сигнала над шумом должно составлять около 10 дБ, для получения удовлетворительного качества факсимильного изображения — приблизительно 35 дБ, качественного телевизионного изображения — более 40 дБ.

В общем случае при уменьшении отношения сигнал/помеха до единицы и менее качество информации настолько ухудшается, что она не может практически использоваться. Для конкретных видов информации и модуляции сигнала существуют граничные значения отношения сигнал/помеха, ниже которых обеспечивается энергетическое скрытие информации.

Так как разведывательный приемник в принципе может быть приближен к границам контролируемой зоны организации, то значения отношения сигнал/помеха измеряются, прежде всего, на границе этой зоны. Обеспечение на границе зоны значений отношения сигнал/помеха ниже минимально допустимой величины гарантирует безопасность защищаемой информации от утечки за пределами контролируемой зоны.

**Маскировка признаков веществ** обеспечивается преобразованием признаков веществ под признаки других веществ, не интересующих злоумышленника. Например, для контрабанды наркотиков иногда их преобразуют в другое химическое вещество, пропускаемое таможенной службой и восстанавливаемое после провоза до первоначального состава.

Другой метод структурного скрытия заключается в трансформации исходного информационного портрета в новый, соответствующий ложной семантической информации или ложной признаковой структуре, и «навязывании» нового портрета органу разведки (злоумышленнику). Такой метод защиты называется **дезинформированием**. Дезинформирование наиболее эффективно при скрытии семантической информации, когда в добытом сообщении содержится ложная информация. При скрытии признаковой информации граница между маскировкой и дезинформированием размытая. Принципиальное различие между ними состоит в том, что маскировка направлена на затруднение обнаружения объекта защиты среди других объектов фона, а дезинформирование — на

создание ложного объекта прикрытия. При поиске орган разведки (злоумышленник) не находит замаскированный объект, при дезинформировании он обнаруживает другой объект вместо истинного, признаки которого невозможно изменить под признаки фона. Например, если в глухом месте без строений размещается шахта стратегической ракеты, то невозможно скрыть подъездные пути автотранспорта к ней. В этом случае структурное скрытие информации о месте нахождения ракетной установки обеспечивается не только маскировкой ее конструкции, но и имитацией функционирования этого объекта.

Дезинформирование относится к числу наиболее эффективных методов защиты информации по следующим причинам:

- создает у владельца защищаемой информации запас времени, обусловленный проверкой разведкой достоверности полученной информации;
- последствия принятых конкурентом на основе ложной информации решений могут быть для него худшими по сравнению с решениями, принимаемыми при отсутствии добываемой информации.

Последняя причина обусловлена тем, что при недостаточности информации увеличивается в пространстве возможных решений область принятия решений, внутри которой находится оптимальное решение. Принятые решения при недостаточности информации будут отличаться от оптимального. При использовании дезинформации может образоваться иная область принятия решений на значительном удалении от оптимального решения. В этом случае могут возникнуть для пользователя ложной информацией катастрофические последствия.

Дезинформирование осуществляется путем подгонки признаков информационного портрета защищаемого объекта под признаки информационного портрета ложного объекта, соответствующего заранее разработанной версии, — **объекта прикрытия**. От тщательности подготовки версии и безукоризненности ее реализации во многом зависит правдоподобность дезинформации. Версия должна предусматривать комплекс распределенных во времени и в пространстве мер, направленных на имитацию признаков ложного объекта. Причем чем меньше при дезинформации исполь-

зуется ложных сведений и признаков, тем труднее вскрыть ее ложный характер.

Различают следующие способы дезинформирования [21]:

- замена реквизитов защищаемых информационных портретов в том случае, когда информационный портрет объекта защиты похож на информационные портреты других «открытых» объектов и не имеет специфических информативных признаков. В этом случае ограничиваются разработкой и поддержанием версии о другом объекте, выдавая в качестве его признаков признаки защищаемого объекта. Например, в настоящее время большое внимание уделяется разработкам продукции двойного применения: военного и гражданского. Распространение информации о производстве продукции сугубо гражданского использования является надежным прикрытием для вариантов военного назначения;
- поддержание версии с признаками, заимствованными из разных информационных портретов реальных объектов. Применяется в тех случаях, когда в организации одновременно выполняется несколько закрытых тем. Путем различных сочетаний признаков, относящихся к различным темам, можно навязать противоположной стороне ложное представление о ведущихся работах без имитации дополнительных признаков;
- сочетание истинных и ложных признаков, причем ложными заменяется незначительная, но самая ценная часть информации, относящейся к защищаемому объекту;
- изменение только информационных узлов с сохранением неизменной остальной части информационного портрета.

Как правило, используются различные комбинации этих вариантов.

Однако этот метод защиты практически сложно реализовать. Основная проблема заключается в обеспечении достоверности ложного информационного портрета. Дезинформирование только в том случае достигнет цели, когда у разведки (злоумышленника) не возникнут сомнения в истинности подсовываемой ему ложной информации. В противном случае может быть получен противоположный эффект, так как при раскрытии разведкой факта дезинформирования полученная ложная информация может сузить область

поиска истинной информации. Учитывая, что потребители информации отчетливо представляют ущерб от дезинформации и при малейших сомнениях будут перепроверять информацию с использованием других источников, дезинформирование в большинстве случаев требует хорошей организации и значительных затрат.

Основу третьего направления инженерно-технической защиты информации составляют методы поиска, обнаружения и нейтрализации источников опасных сигналов. Так как эти источники обнаруживаются по их демаскирующим признакам, то эти методы содержат процедуры идентификации источников случайных опасных сигналов по их демаскирующим признакам.

### Вопросы для самопроверки

1. Основные факторы, влияющие на эффективность защиты информации от угроз воздействия.
2. Условия, которые необходимо выполнить для обнаружения и распознавания объекта разведки.
3. Чем отличаются процедуры обнаружения от процедур распознавания?
4. Основные направления инженерно-технической защиты информации.
5. Методы инженерно-технической защиты информации.
6. Чем отличается инженерная защита объектов от их технической охраны?
7. Условие эффективного обеспечения временного скрытия объектов защиты.
8. Что представляет собой информационная модель объекта защиты?
9. Чем маскировка отличается от дезинформирования?
10. Условие эффективного энергетического скрытия.

# Глава 9. Методы физической защиты информации

## 9.1. Категорирование объектов защиты

Объектами физической защиты являются материальные ценности, в том числе источники защищаемой информации, а также контролируемые зоны, в которых расположены эти материальные ценности. Объекты делятся на **стационарные** и **мобильные**. К стационарным объектам относятся территория, здания, сооружения, помещения, протяженные рубежи. Мобильные объекты включают временные стоянки, транспортные средства, малогабаритные объекты. Объекты описываются набором административно-правовых, инженерно-технических, организационных, специальных характеристик. Специальные характеристики описывают объект с точки зрения его безопасности. Объекты охраны (защиты) разделяются на 3 категории, указанные в табл. 9.1.

Во вневедомственной охране МВД РФ используется расширенная классификация объектов:

- В1 — особо важные объекты с повышенной стоимостью ценностей или повышенной значимостью потерь;
- В2 — особо важные объекты;
- В3 — важные объекты;
- В4 — простые объекты;
- В5 — простые объекты с пониженной стоимостью или значимостью ценностей.

При этом объекты категории А включают объекты категорий В1 и В2, Б — категории В3, С — объекты категорий В4 и В5.

*Таблица 9.1*

| *Категория* | *Наименование категории* | *Назначение или принадлежность объекта* | *Последствия от реализации угроз* |
|---|---|---|---|
| А | Особо важные объекты | Хранилища и депозитарии банков; предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы | Особо крупный или невосполнимый материальный ущерб, экологическая катастрофа на объекте или в регионе, гибель или угроза жизни большому числу людей на объекте или в регионе, политические последствия, потеря особо важных государственных секретов, другие особо тяжкие последствия |
| Б | Важные объекты | Кассовые залы банков; подъезды инкассаторских машин; помещения для хранения и работы с важной защищаемой информацией; торговые центры по продаже ценных товаров; производственные помещения для изготовления ценной продукции | Значительный материальный или финансовый ущерб, угроза здоровью или жизни людей, потеря государственных или важных коммерческих секретов |
| В | Простые (обычные) объекты | Торговые залы магазинов; служебные помещения учреждений; офисы среднего и малого бизнеса; производственные помещения общего назначения; жилые помещения | Материальный или финансовый ущерб; информационный ущерб коммерческого или служебного рода; нарушение комфортности личной жизни или служебной деятельности |

Категорирование объектов позволяет систематизировать разнообразные требования к объектам защиты и сформулировать их в виде нормативов. Например, применительно к категориям объектов вневедомственной охраны МВД РФ нормативные характеристики деятельности этих органов приведены в табл. 9.2 [22].

*Таблица 9.2*

| *Выполняемые мероприятия* | *Категории объектов* | | | | |
|---|---|---|---|---|---|
| | *B1* | *B2* | *B3* | *B4* | *B5* |
| Время передачи извещений с объекта группе захвата, не более мин. | 1 | 1,5 | 2 | 2,5 | 3 |
| Время прибытия группы захвата к объекту, не более мин. | 2,5 | 3,5 | 5 | 10 | 15 |

## 9.2. Характеристика методов физической защиты информации

Методы физической защиты источников информации должны обеспечивать:

- задержку злоумышленника или иного источника угрозы на время, большее времени нейтрализации угрозы;
- обнаружение злоумышленника или источника иной угрозы;
- нейтрализацию угроз воздействия на источник информации.

Известно, что самый экономичный путь нейтрализации неприятностей — их предупреждение. При эксплуатации технических средств оно достигается их профилактическим обслуживанием. Органы правопорядка проводят профилактику преступлений. Система защиты в своем составе также должна иметь механизмы профилактики вторжений в нее источников угроз воздействий. В качестве таких профилактических мер могут использоваться:

- «демонстрация силы»;
- распространяемые среди сотрудников организации легенды о задержании нарушителей, проникших на территорию организацию.

«Демонстрация силы» — широко распространенный в природе и в обществе метод предупреждения противника о собствен-

ной силе. При обострении отношений между двумя странами в них проводятся военные учения, которые должны продемонстрировать противоположной стороне свою военную мощь. «Демонстрация силы» подсистемой физической защиты проявляется в виде предоставления злоумышленнику возможности наблюдения средств механической защиты. Вид трудно преодолеваемых средств физической защиты может заставить злоумышленника отложить проникновение или отказаться от него вообще. В этом случае время задержки системой злоумышленника возрастает до момента следующей попытки проникновения.

Если злоумышленник решается на проникновение, то скорость его продвижения зависит от длины пути от места вторжения до места нахождения источника, количества и прочности механических препятствий на этом пути. Возможны различные варианты обеспечения требуемого времени задержки путем различных сочетаний количества рубежей (на границах зон) и их укрепленности. Одно и то же время задержки обеспечивается небольшим количеством хорошо укрепленных рубежей и большим количеством более слабых рубежей. Рациональный вариант находится в результате минимизации стоимости. Однако следует учитывать возможность помощи завербованных сотрудников внешнему злоумышленнику. Чем больше используется мер защиты, тем сложнее сотруднику их выявить и передать сведения о них злоумышленнику.

Если источник информации хранится в сейфе помещения, то злоумышленнику в типовом варианте необходимо преодолеть забор, стены (двери, окна) здания, дверь коридора, если она закрывается во внерабочее время, дверь помещения, сейф. Механическая прочность каждой из этих преград оценивается временем их преодоления при использовании различных инструментов. Например, для взлома сейфа со средней взломоустойчивостью (V класс) с использованием лома, кувалды и зубила требуется в среднем 22 мин, газового резака — 14,1 мин, а колонкового бура с алмазной коронкой — 8,7 мин [22].

Пример времени преодоления преград в помещениях квалифицированным злоумышленником, оснащенным техническими средствами, указан в табл. 9.3 [23].

*Таблица 9.3*

| *№ п/п* | *Вид преграды и ее параметры* | *Время преодоления, с* |
|---|---|---|
| 1 | Окно (толщина стекла 4 мм) | 9–12 |
| 2 | Окно с металлической решеткой (пруток d = 20 мм) | 150–170 |
| 3 | Дверь деревянная | 12–15 |
| 4 | Дверь деревянная, обитая железом | 90–110 |
| 5 | Дверь металлическая, решетка (пруток d = 20 мм) | 120–150 |
| 6 | Дверь сплошная металлическая (лист толщиной 4 мм) | 300–400 |
| 7 | Перегородка кирпичная толщиной 15 см | 90–100 |
| 8 | Стена кирпичная толщиной 30 см | 400–450 |
| 9 | Висячий замок | 15–25 |
| 10 | Накладной замок | 20–30 |
| 11 | Шкаф металлический (лист 2 мм) | 70–90 |

С целью увеличения времени задержки злоумышленника и уменьшения времени нейтрализации угроз целесообразны следующие меры:

- удаление на максимально возможное расстояние от забора мест нахождения источников с наиболее ценной информацией;
- размещение мест нахождения дежурной смены возле помещений с ценной информацией;
- установка дополнительных рубежей защиты на наиболее вероятных путях движения злоумышленника к местам хранения ценной информации;
- создание свободных от растительности полос и хорошо просматриваемых (зон) по обеим сторонам забора;
- повышение механической прочности забора, стен, дверей и окон на первом этаже зданий, люков в подвальные помещения, дверей коридоров и помещений, сейфов и хранилищ.

Задержка распространения огня как второй по значимости угрозы для источника информации достигается:

- постоянным контролем за проводами и коммутационными устройствами (сетевыми розетками и вилками, предохранителями и автоматами) цепей электропитания, оперативная замена проводов с нарушенной или потрескавшейся изоляцией, а также нагревающихся электророзеток и вилок;

- удалением из помещений, в которых хранится ценная информация, электронагревательных приборов с открытыми теплоэлектронагревательными устройствами (ТЭНами) и легковоспламеняющихся веществ и материалов;
- применением пожароустойчивых сейфов и хранилищ.

Однако при оснащенности злоумышленника современными инструментами нельзя обеспечить его задержку на длительное время, например до прихода сотрудников на работу. Также невозможно сохранить носители информации, находящиеся вблизи очага пожара, без своевременного его тушения.

Поэтому существенное влияние на эффективность физической защиты оказывают показатели обнаружения и нейтрализации угроз.

Возможность обнаружения угрозы оценивается тремя вероятностями:

- вероятностью правильного обнаружения (угроза есть) — $P_{оу}$;
- вероятностью необнаружения угрозы при ее наличии — $P_{ну}$;
- вероятностью ложного обнаружения угрозы (угроза отсутствует) — $P_{лу}$.

Как правило, $P_{оу} >> P_{ну}$ и $P_{оу} >> P_{лу}$, а сумма значений этих вероятностей равна 1. Ошибки необнаружения и ложного обнаружения называют также ошибками 1-го и 2-го рода соответственно. Ошибки 1-го и 2-го родов имеют различные неприятные последствия. Наибольшей ущерб могут создать ошибки 1-го рода, так как злоумышленник или огонь в случае их необнаружения могут добраться до источника информации. Так как в общем случае вероятность обнаружения угроз зависит от количества и информативности их демаскирующих признаков, то для обнаружения используются их прямые и косвенные признаки. Прямыми признаками злоумышленника, на которые реагируют современные датчики (извещатели), являются:

- вес взрослого человека 40–100 кг;
- рост взрослого человека 140–200 см;
- непрозрачность или слабая прозрачность тела человека для оптических и радио- (в СВЧ-диапазоне) электромагнитных лучей;
- инфракрасное излучение;
- скорость движения в диапазоне 1–9 м/с;

- действия человека, направленные на преодоление или разрушение преград.

Реакция преград на действия злоумышленника образует его косвенные признаки: вибрация заборов из сетки, стен, стекол, звуки стекол при разбитии и др.

Признаковая структура пожара описывается набором следующих признаков:

- дым и задымленность помещения;
- ультрафиолетовое излучение;
- инфракрасное излучение с уровнем излучения выше фона.

Информативность рассмотренных признаков зависит от времени их проявления и фоновых значений. В рабочее время информативность признаков злоумышленника мала, в ночное время может быть близкой к 1. Например, появление в пустом коридоре ночью постороннего человека почти равнозначно появлению злоумышленника. Температура в замкнутом пространстве в жаркое время может приблизиться к температуре срабатывания пожарного извещателя. Кроме того, на извещатель могут действовать, даже в течение очень короткого времени, различные помехи с признаками, которые он не отличает от признаков источников угроз.

К типовым помехам, признаки которых могут быть близки признакам угроз, относятся:

- животные и насекомые, попадающие в зону контроля извещателя;
- вибрация ограждений помещения, вызванных движением тяжелого автотранспорта по улице, строительными работами во дворе, работой электромеханических средств (мощных холодильников, вентиляторов, кондиционеров и др.), ураганом, землетрясением и другими явлениями;
- ветки и стволы деревьев, наружные светильники и др., колеблющиеся под действием ветра;
- инфракрасные излучения Солнца, фар проезжающих автомобилей, батарей отопления и других нагревателей воздуха;
- мощные электромагнитные излучения электрических и радиоустановок;
- падающие листья, дождь, снег.

Ложная тревога не приводит к изменению защищаемой информации, она достаточно просто выявляется путем осмотра места

размещения извещателя, проверки его работоспособности, анализа причин ложной тревоги и их устранения. Но частое ложное срабатывание извещателей оказывает психологическое воздействие на дежурную смену, затормаживая их реакцию на последующие сигналы тревоги. В зарубежном боевике даже обыгрывается сценарий, когда грабители путем многократного создания ложных тревог в банке усыпили бдительность полицейских и без проблем проникли в хранилище. Можно предположить, что если ложное срабатывание происходит не чаще одного раза в месяц, то у операторов не возникает психологического привыкания к нему.

Повышение вероятности правильного обнаружения злоумышленника и пожара и уменьшение вероятности ложной тревоги достигается:

- совершенствованием примененных в извещателях технических решений;
- выбором извещателей, наиболее эффективных для конкретных условий;
- установкой извещателей в местах контролируемой зоны с минимальным уровнем помех;
- совместным применением n извещателей, обнаруживающих разные признаки источников угроз.

При совместном применении разных извещателей сигнал тревоги формируется по определенному логическому правилу принятия решения, которое в общем виде можно сформулировать как «m из n», т. е. сигнал тревоги формирует при срабатывании любых m из n извещателей. Если m = 1, то правило соответствует известному логическому условию «или», когда m = n — условию «и». Правило «или» обеспечивает максимальную вероятность как правильного обнаружения, так и ложного срабатывания, правило «и» минимизирует эти вероятности. Другие варианты обеспечивают промежуточные результаты.

Действительно, при реализации правила «или» сигнал тревоги возникает при обнаружении признака источника угрозы или помехи хотя бы одним из n извещателей. Например, если на рубеже защиты установлены 3 извещателя, реагирующие на разные признаки источника угроз с вероятностью 0,95, 0,9 и 0,85, то вероятность обнаружения тремя извещателями хотя бы одного из признаков возрастает до величины 0,993. Но это значение включает

также вероятность появления ложного сигнала тревог под действием помех. Если принять, что вероятности ложного срабатывания этих извещателей равны 0,1, 0,07 и 0,05, то при совместном использовании 3 извещателей по правилу «или» суммарная вероятность ложного срабатывания увеличится до 0,2. Следовательно, суммарная вероятность правильного обнаружения примет значение 0,993–0,2 = 0,793, что менее значения вероятности правильного приема любого из рассмотренных извещателей. Для правила «и» при этих же исходных данных вероятность обнаружения угрозы снизится до величины 0,73, но вероятность ложного срабатывания станет очень малой — $3{,}5 \cdot 10^{-4}$.

Учитывая, что ущерб при пропуске злоумышленника и пожара существенно выше, чем ложное срабатывание извещателей от помех, предпочтение отдается правилу принятия решения «или». Уменьшение вероятности ложной тревоги достигается комплексными мерами, предусматривающими усложнение эталонной признаковой структуры извещателей, их грамотным выбором и использованием.

Своевременность обнаружения характеризуется соотношением времени $\tau_п$, необходимого для проникновения злоумышленника или иного источника угрозы до источника информации после их обнаружения (без нейтрализации), и времени $\tau_р$, необходимого для их нейтрализации. Своевременность нейтрализации угрозы можно оценить безразмерной величиной в интервале 0–1, равной отношению $(\tau_п - \tau_р) / \tau_п$ при $\tau_п > \tau_р$ и 0 — при обратном соотношении времен.

Время продвижения злоумышленника к источникам информации, вероятность его обнаружения и время его задержания зависят также от освещенности рубежей защиты и контролируемых зон в темное время суток и при плохих погодных условиях. В интересах защиты применяют три вида освещения: **дежурное, охранное** и **аварийное**.

**Дежурное освещение** повышает освещенность объектов, рубежей защиты и контролируемых зон в темное время суток и при плохой погоде до уровня, необходимого для визуального наблюдения и наблюдения с помощью телевизионных средств. Чрезмерная освещенность требует значительного ресурса. Кроме того, нераци-

онально выполненное дежурное освещение способствует изучению злоумышленником системы защиты и упрощает проникновению его к источнику информации.

**Охранное извещение** предназначено для увеличения освещенности участков рубежей и зон, из которых поступили сигналы тревоги. В обычном режиме (при отсутствии нарушений) охранное освещение выключено. Оно должно обеспечить [24]:

- равномерную освещенность охраняемой зоны шириной 3–4 м;
- возможность автоматического включения освещенности на отдельном участке при срабатывании сигнала тревоги от извещателя, установленного на этом участке;
- управления работой средств освещения из помещения контрольно-пропускного пункта (КПП);
- совместимость с техническими средствами охранной сигнализации и охранного телевидения;
- непрерывность работы на КПП и постах охраны.

**Аварийное освещение** предназначено для обеспечения минимального освещения на опасных участках рубежей и зон при нарушении в результате действий злоумышленника, стихии и технической неисправности нормального энергоснабжения системы защиты от сети 220/380 В. Аварийное освещение включается автоматически или вручную и должно обеспечить не менее 5% освещенности при охранном освещении.

Определить задержку злоумышленника и пожара можно суммированием временных показателей рубежей, которые эти источники угроз должны преодолеть до физического их контакта с источниками информации.

Эффективность физической защиты зависит также от способа и времени нейтрализации угроз. Заставить злоумышленника отказаться от своих намерений можно путем психологического и физического воздействия сил нейтрализации. Психологическому воздействию подвержены неподготовленные злоумышленники. Сплошной бетонный забор с колючей проволокой и укрепленными на нем средствами технической охраны, металлические двери и забор СКУД и другие признаки мощной защиты организации могут остановить непрофессионального злоумышленника. Мощное психологическое воздействие даже неподготовленного злоумыш-

ленника оказывают средства тревожной сигнализации в виде звука большой громкости (100–120 дБ) и яркого света прожектора, включаемых в ночное время после его обнаружения.

Подготовленного злоумышленника останавливают с помощью сил и средств охраны. Типовыми силами нейтрализации злоумышленника являются:

- в автономных подсистемах физической защиты — сотрудники службы безопасности, в отдельных фирмах с очень крупным капиталом они усиливаются сотрудниками подразделения быстрого реагирования;
- в централизованных подсистемах физической защиты — сотрудниками вневедомственной охраны.

Охранники могут оснащаться резиновыми дубинками, электрошоковыми устройствами, газовым и огнестрельным гладкоствольным и нарезным оружием. Обнаруженные злоумышленники задерживаются охранниками и должны передаваться для проведения оперативно-следственных действий правоохранительным органам или органам ФСБ РФ.

Нейтрализация (устранение) пожара обеспечивается автономными силами и средствами организации, а также нарядами пожарной службы МЧС. В любой организации должен быть штатный или внештатный пожарник, обязанный контролировать соблюдение сотрудниками организации правил противопожарной безопасности, работоспособность средств пожаротушения и сроки их проверки.

Основные направлениями повышения эффективности пожаротушения:

- совершенствование традиционных и создание новых огнетушащих веществ;
- автоматизация процессов пожаротушения.

Свойства такого традиционного огнетушащего средства как вода существенно изменяются в результате введения в нее специальных добавок. Эти добавки увеличивают смачиваемость водой материалов в зоне пожара, повышают ее текучесть в трубопроводах и пожарных шлангах, уменьшают температуру замерзания воды. Тонко распыляемая под большим давлением вода существенно лучше изолирует горючее вещество от кислорода воздуха и не

причиняет вреда окружающим очаг пожара предметам и материалам.

Кроме воды в качестве огнетушащих веществ все шире применяются пена, нейтральные для человека газы, порошки.

Так как при тушении пожара важна каждая минута, а человек как элемент управления может в момент возгорания отсутствовать или растеряться, то автоматизация пожаротушения рассматривается как основное направление повышения его эффективности. Автоматизация достигается передачей все большего числа функций по обнаружению и нейтрализацию пожара автоматическим устройствам. За человеком остаются функции контроля и принятия решения о включении средств автоматического пожаротушения и вызова пожарной команды. В централизованных системах охраны сигнал тревоги передается на пульт дежурного отделения МЧС.

### Вопросы для самопроверки

1. Категории объектов защиты (охраны).
2. Задачи физической защиты информации.
3. Профилактические меры, применяемые в системе защиты информации для уменьшения вероятности вторжения злоумышленников.
4. Пути увеличения времени задержки источника угроз и уменьшения времени реакции системы на угрозы.
5. Демаскирующие признаки злоумышленника и пожара.
6. Как оценивается возможность обнаружения угрозы?
7. Способы повышения вероятности обнаружения источников угроз и минимизации ошибок.
8. Преимущества и недостатки автономных и централизованных систем охраны.

# Глава 10. Методы противодействия наблюдению

## 10.1. Методы противодействия наблюдению в оптическом диапазоне

При защите информации от наблюдения в оптическом диапазоне необходимо учитывать факторы, влияющие на вероятность обнаружения (распознавания) объектов наблюдения и ухудшающие точность измерения видовых демаскирующих признаков. Эффективность поиска объектов наблюдения зависит от:

- яркости объекта;
- контраста объект/фон;
- угловых размеров объекта;
- угловых размеров поля обзора;
- времени наблюдения объекта;
- скорости движения объекта.

**Яркость объекта** на входе оптического приемника определяет мощность носителя, превышение которой над мощностью помех является необходимым условием получения изображения с необходимым качеством. Современные приемники имеют чувствительность, соответствующую энергии нескольких фотонов.

**Контрастность объекта** с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания. Различают яркостной и цветовой контраст. Яркостной контраст $К_я$ определяют как отношение разности яркости объекта и фона к яркости объекта или фона:

$$К_я = (В_о - В_ф)/В_о,\ В_о > В_ф \quad \text{или} \quad К_в = (В_ф - В_о)/В_ф,\ В_ф > В_о,$$

где $В_о$ и $В_ф$ — яркость объекта и фона соответственно.

Относительная разность яркостей отдельных спектральных составляющих света от объекта и фона характеризует их **цветовой** контраст. В видимом и ближнем диапазонах света яркостной контраст на входе оптической системы средства добывания несколько снижается за счет яркости дымки, которую можно рассматривать как помеху. В дальних зонах инфракрасного излучения яркость дымки не оказывает существенного влияния на изменение этого

контраста. Контраст может принимать значения в диапазоне 0–1. При $К_я$ = 0,08–0,1 объект почти сливается с фоном и плохо различается на фоне. Значения цветового контраста объектов и фона могут существенно отличаться в разных длинах волн, что используется в зональной (через цветовые фильтры) аэрофотосъемке.

При поиске объекта его форма не играет большой роли, а имеет значение только его площадь в пределах соотношения сторон от 1:1 до 1:10. Увеличение **угловых размеров** объекта в 2 раза сокращает время, необходимое для его обнаружения, в 8 раз.

Время для обнаружения объектов светлее и темнее фона при одинаковых абсолютных значениях контраста примерно одинаковое. С увеличением яркости фона время поиска объекта наблюдателем уменьшается, так как увеличивается разрешающая способность и контрастная чувствительность глаза. Если яркость фона чрезмерно велика, то возникают дискомфорт и ослепление, ухудшающие разрешение и контрастную чувствительность глаза.

С увеличением **поля обзора** увеличивается и время, необходимое для поиска объекта: двукратное увеличение поля обзора повышает время поиска в 4 раза. При этом время поиска определяется не формой поля, а его угловыми размерами.

Поиск движущихся объектов имеет свои особенности: движение ухудшает видимый контраст объекта, величина которого зависит не только от угловой скорости, но и от угловых размеров объекта наблюдения. Чем меньше угловой размер объекта, тем больше влияние **скорости** на время и вероятность обнаружения объекта. Объекты, движущиеся с малой скоростью, обнаруживаются легче, чем неподвижные, а движущиеся с большой скоростью — труднее из-за ухудшения видимого контраста.

Следовательно, в интересах защиты информации об объекте (его демаскирующих признаков) необходимо уменьшать контраст объект/фон, снижать яркость объекта и уменьшать угловые размеры объекта, не допуская наблюдателя близко к объекту. Мероприятия, направленные на уменьшение величины контраст/фон, называются **маскировкой**.

С учетом этих факторов и общих методов инженерно-технической защиты информации методы защиты информации от наблюдения в оптическом диапазоне указаны на рис. 10.1.

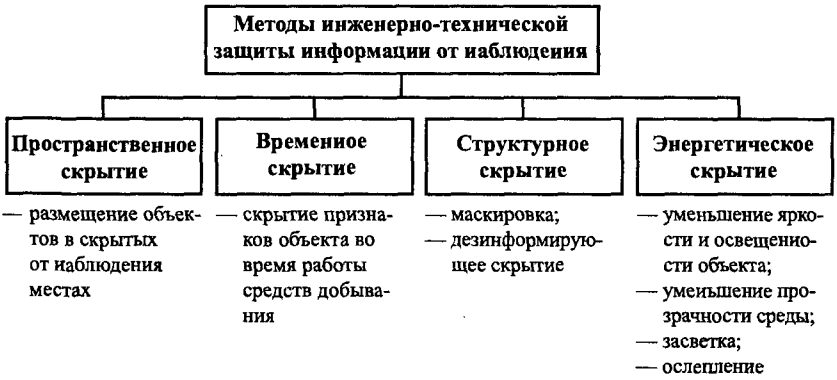



*Рис. 10.1.* Методы защиты информации от наблюдения

Пространственное скрытие обеспечивается размещением объектов защиты в точках (местах) пространства, неизвестных злоумышленнику или недоступных для наблюдения. С этой целью предприятия военно-промышленного комплекса размещали подальше от границ Советского Союза, а районы их нахождения объявлялись зонами, закрытыми для посещения иностранцами. Также для выделенных помещений в здании выбираются комнаты в отсеках с ограниченным допуском в них сотрудников.

Если время наблюдения известно, то достаточно эффективной мерой является перевод объекта наблюдения в состояние, в котором не проявляются видовые признаки в течение времени наблюдения. Например, при подлете разведывательного КА к полигону, на котором испытывается новая военная техника, работы, в ходе выполнения которых проявляются видовые демаскирующие признаки, прекращаются до момента выхода КА из зоны наблюдения.

**Маскировка** представляет собой метод структурного скрытия объекта защиты путем изменения его видовых признаков под признаки других объектов (фона). Применяются следующие способы маскировки:

- использование маскирующих свойств местности;
- маскировочная обработка местности;
- маскировочное окрашивание;
- применение искусственных масок;
- нанесение на объект воздушных пен.

Использование маскирующих свойств местности (неровностей ландшафта, складок местности, холмов, гор, стволов и кроны деревьев и т. д.) является наиболее дешевым способом скрытия объектов. Однако для реализации этого способа необходимо наличие в месте нахождения объекта соответствующих естественных масок. Кроме того, маскирующие возможности растительности зависят от времени года. Эффективность маскировки оценивается отношением площади, закрываемой, например, деревьями к площади наблюдаемой зоны.

Если отсутствуют или недостаточны для маскировки природные условия, то возможна дополнительная обработка местности, повышающая ее маскирующие возможности. Она состоит в дернировании (укладке дерна) и посеве травы, создании изгородей из живой растительности, в механической и химической обработке участков местности — распятнении. Обработка местности направлена на изменение фона под основной цвет объекта: на зеленый при дернировании и посеве травы или другой цвет (бурый с различными оттенками, соломенно-желтый) при распятнении.

**Распятнение** достигается расчисткой поверхности почвы от дерна с помощью машин или химическим путем — солями (железным и медным купоросом, бертолетовой солью и др.) и гербицидами. Этот способ имеет ограниченное применение в связи с большой задержкой проявлений маскировочных свойств местности после обработки и вредным воздействием на природу. Например, трава вырастает через несколько недель после посева, а цвет растительности меняется через несколько дней после ее химической обработки.

Маскировочная обработка местности эффективна для скрытия наземных объектов и фона при наблюдении сверху, например, летного поля аэродрома для легких самолетов и вертолетов.

**Маскировочное окрашивание** применяется для изменения цвета объекта, маски или фона и производится путем:

- поверхностной окраски, при которой красочный слой наносится на окрашиваемую поверхность;
- глубинной окраски, при которой краситель пропитывает окрашиваемый материал (ткани, маскировочной сети) или вводятся

пигменты при изготовлении материала (цветных цемента, штукатурки, пластмассы и др.).

При поверхностной окраске применяются различные краски, лаки, эмали, битумы, пасты, при глубинной окраске — синтетические красители, порошкообразные пигменты и крупнофракционные цветные материалы (песок, молотые руды).

Различают три вида маскировочного окрашивания:

- защитное;
- деформирующее;
- имитационное.

**Защитное окрашивание** поверхности объекта проводится одноцветной краской под цвет и среднюю яркость фона окружающей местности и предметов возле маскируемого объекта. Цвета защитного окрашивания: хаки, желтовато-серый, серо-зеленоватый, голубовато-серый, оливковый относятся к так называемым универсальным, которые плохо выделяются на фоне разнообразных объектов, прежде всего ландшафта. Однотонный желто-сероватый цвет полевого обмундирования солдат армий многих государств был плохо заметен на растительном, горном, пустынном, городском фонах. Приблизительно такими же возможностями обладал грязно-зеленовато-серый цвет немецкого обмундирования во Второй мировой войне. Защитная окраска оливкового или зеленовато-грязного цвета использовалась как заводская для военной техники.

**Деформирующее окрашивание** предусматривает нанесение на поверхность объекта пятен неправильной геометрической формы 2–3 цветов, имитирующих световые пятна окружающей среды. Различают мелкопятнистую (дробящую) и крупнопятнистую (искажающую контуры) деформирующую окраску. Края цветовых пятен могут быть резко очерченными или расплывчатыми. Деформирующее окрашивание психологически искажает образ защищаемого объекта у наблюдателя и затрудняет обнаружение и распознавание им объекта по признакам его формы. Оно в настоящее время является основным видом маскировки военнослужащих и военной техники армий большинства стран. Выпускается достаточно большое количество вариантов камуфляжа для разных времен года и типов местности. Наряду с маскировочными комбине-

зонами применяют маскировочные маски для лица или грим, которые наносят на лицо и руки и которые входит в состав маскировочного комплекта войск специального назначения. Деформирующая окраска труднее поддается дешифрованию на пестрых фонах и обеспечивает меньшую вероятность обнаружения и опознавания маскируемых объектов.

При **имитационном окрашивании** цвет и характер пятен на поверхности объекта подбираются под расцветку окружающей местности, объектов или предметов в месте расположения защищаемого объекта. Как правило, этот вид окрашивания применяется для неподвижных объектов: долговременных огневых сооружений, зданий, гидротехнических сооружений и др. В результате маскируемый объект сливается с окружающей местностью или приобретает внешний вид другого объекта. Например, взлетно-посадочная полоса военного аэродрома может быть раскрашена под обычное шоссе или грунтовую дорогу с расположенными возле нее зданиями или иными объектами.

**Маскировочное окрашивание** просто реализуется, но эффект маскировки зависит от сезонных и иных изменений окружающей среды. Кроме того, частое перекрашивание объекта требует больших материальных и временных затрат.

Для маскировки без окрашивания создаются специальные конструкции — искусственные оптические маски, снижающие яркостной и цветовой контраст объекта защиты и фона.

**Энергетическое скрытие** демаскирующих признаков объектов достигается путем:

- уменьшения яркости источников света объекта или освещенности объекта внешними источниками;
- снижения прозрачности среды распространения света от объекта наблюдения до злоумышленника или его технического средства;
- засветки изображения объекта посторонними световыми лучами — помехами;
- ослепления зрительной системы наблюдателя или светоприемника.

Первые два метода относятся к пассивным и приводят к уменьшению уровня светового сигнала на входе оптического приемни-

ка. Так как его светочувствительные элементы имеют собственные шумы, то при уровне сигнала ниже собственных шумов обнаружение и распознавание его становятся невозможными.

К активным методам энергетического скрытия относятся **засветка изображения** или **ослепление светочувствительного приемника**. Засветка возникает, когда изображение помехи накладывается на изображение объекта и фона. При этом уменьшается контраст изображения по отношению к фону. Действительно, при условии, что $B_о > B_ф$ контраст изображения с учетом яркости $B_п$, создаваемой на фотографии и экране монитора помехой, равен величине

$$K_{ял} = \frac{B_о + B_п - (B_ф + B_п)}{B_о + B_п} = \frac{B_о - B_ф}{B_о + B_п},$$

где $B_о$ и $B_ф$ — значение яркости объекта и фона соответственно.

С увеличением мощности помехи (яркости $B_п$) контраст $K_{ял} \to 0$.

Засветка происходит, когда солнечные лучи попадают на экран монитора компьютера или при наблюдении объектов через освещаемые светом стекла окон помещения или салона автомобиля. При наблюдении через стекло изображение формируется суммой лучей, отраженных от объектов наблюдения и от стекла. Свет от стекла представляет собой помеху. Световой поток от объекта наблюдения уменьшается стеклом, вследствие чего яркость помехи становится больше яркости объекта и фона. Эту разницу увеличивают применением тонированных (затемненных) или «зеркальных» (с алюминиевым или медным напылением) стекол. Тонированные стекла уменьшают $B_о$ и $B_ф$, а «зеркальные» увеличивают $B_п$. В результате этого контрастность объекта наблюдения уменьшается до величин, при которых объект на виден.

При превышении мощности помехи на входе приемника значения, соответствующего его динамическому диапазону, возникают искажения информации вплоть до ее полного разрушения. Чрезмерно большая мощность помехи может привести к необратимым изменениям в светочувствительных элементах. Например, высокочувствительные телевизионные камеры, позволяющие наблюдать за обстановкой при очень малом освещении, могут вый-

ти из строя при попадании на ПЗС-матрицу прямых лучей солнечного света.

Классическим примером ослепления может служить применение наступающими советскими войсками ночью в Берлинской операции 1945 г. 142 прожекторов, свет которых лишил фашистов возможности видеть наступающие войска и эффективно обороняться. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают естественные и искусственные маски, а также аэрозоли в среде распространения.

Так как спектральные характеристики объектов и среды различаются для видимого и ИК-диапазонов, то при организации защиты информации от наблюдения в оптическом канале необходимо учитывать диапазон частот носителя информации. Хотя параметры средств визуально-оптического наблюдения (по разрешению, дальности, цвету изображения) в ИК-диапазоне значительно более низкие, чем в видимом, но при наблюдении в нем появляется дополнительный демаскирующий признак объектов, не обнаруживаемый в видимом, — температура поверхности объекта относительно температуры фона.

Естественный фон в ИК-диапазоне можно рассматривать как сложный источник ИК-излучения, характеристики которого зависят от условий освещения, географической широты и долготы, сезона и температуры среды, метеоусловий, природы подстилающей поверхности, времени года и дня и т. п. Отражающая способность ряда природных фонов, таких как трава и листва деревьев, возрастает со смещением максимума излучений в область более длинных волн. Например, отражающая способность травы и листвы в диапазоне волн 0,76–12 мкм выше отражающей способности в видимом диапазоне приблизительно в 5–10 раз, коры — в 3–5 раз. Поэтому объекты, окрашенные маскирующей краской для видимого диапазона, могут хорошо наблюдаться в ИК-диапазоне. Следовательно, при выборе краски необходимо учитывать характер изменения ее

коэффициента отражения от длины волны падающего на объект света, в том числе и в ИК-диапазоне.

Кроме того, на яркость объекта с собственными источниками тепла и, следовательно, на его контраст с фоном в ИК-диапазоне влияет температура поверхности объекта. Для его информационной защиты применяются различные теплоизолирующие экраны, в том числе листья деревьев и кустарников, сено, брезент и др. материалы. Хорошими теплоизолирующими свойствами обладают воздушные пены.

## 10.2. Методы противодействия радиолокационному и гидроакустическому наблюдению

Специфика защиты от радиолокационного наблюдения вызвана особенностями получения радиолокационного изображения. Структура радиолокационного изображения зависит от разрешающей способности радиолокатора, электрических свойств отражающей поверхности объектов и фона, от степени ее неровностей (шероховатости), от длины и поляризации волны, облучающей объект, угла падения электромагнитных волн на поверхность объекта. Разрешающая способность локатора определяется в основном шириной диаграммы направленности его антенны, как известно, совмещающей в одной конструкции функции передающей и приемной.

В настоящее время наиболее широко используется для радиолокации см-диапазон. Разрешение на местности в этом диапазоне самолетных (бортовых) радиолокаторов составляет единицы метров. С целью повышения разрешающей способности радиолокаторов применяется мм-диапазон, в котором проще создать антенны приемлемых размеров с более узкой диаграммой направленности. Но мм-волны сильнее затухают в атмосфере, что приводит к снижению дальности наблюдения. Кроме того, более длинные волны имеют лучшую проникающую способность в поверхность объекта, что затрудняет его маскировку.

Таким образом, радиолокационное изображение существенно отличается от изображения в оптическом диапазоне и использует-

ся разведкой для получения дополнительных демаскирующих признаков на существенно большем удалении от объекта и в неблагоприятных климатических условиях. Указанные особенностей учитываются при организации защиты информации. Меры по защите направлены на снижение ЭПР объекта в целом и его характерных участков, содержащих информативные демаскирующие признаки.

Структурное скрытие обеспечивается в результате изменения структуры изображения защищаемого объекта на экране локатора путем:

- покрытия объекта экранами, изменяющими направления распространения отраженного электромагнитного поля;
- размещения в местах расположения объекта дополнительных отражателей;
- генерирования радиопомех.

В качестве дополнительных радиоотражателей применяются уголковые, линзовые, дипольные отражатели и переизлучающие антенные решетки (ПАР).

Для энергетического скрытия объектов от радиолокационного наблюдения его поверхность покрывают материалами, обеспечивающими **градиентное** и **интерференционное поглощение облучающей электромагнитной энергии**.

Другой способ энергетического скрытия, который широко применяется для защиты объектов от радиолокационного наблюдения, — **генерация помех**. Простейшей помехой является гармоническое колебание на частоте РЛС, создаваемое генератором помех в месте нахождения защищаемого объекта. Так как диаграмма направленности антенны РЛС имеет, как правило, боковые лепестки, то такая помеха создает шумовую засветку экрана локатора.

Более сложной по структуре является модулированная помеха с одним или несколькими изменяющимися параметрами. Модулированная помеха бывает **непрерывной** и **импульсной** и обладает спектром, близким к спектру излучения РЛС. По эффекту воздействия помехи разделяются на маскирующие изображение объекта путем зашумления экрана РЛС и имитирующие на нем ложные световые пятна. Изменяя структуру и время задержки имитационной помехи, можно менять форму, место и характер движения ложной засветки на экране локатора.

Защита информации об объектах, находящихся в воде, предусматривает, прежде всего, защиту от гидроакустического наблюдения. Способы этой защиты по сути соответствуют рассмотренным с учетом особенностей канала утечки. В качестве основных применяются следующие:

- маскировка с использованием природных явлений. При перепаде температуры слоев возникают акустические экраны, трудно преодолимые для акустических излучений;
- использование звукопоглощающих покрытий сотовой конструкции из нейлона, полиэтилена, полипропилена и различных пластмасс, а также содержащих натуральный каучук. За рубежом проводятся опыты по покрытию корпусов подводных лодок материалами, поглощающими до 90% акустической энергии;
- создание активных помех гидролокаторам, в том числе путем ретрансляции облучающих сигналов с усилением их мощности.

### Вопросы для самопроверки

1. Факторы, влияющие на эффективность поиска объектов наблюдения.
2. Способы маскировки объектов наблюдения.
3. Виды маскировочного окрашивания.
4. Различия в механизме маскировки защитного и деформирующего окрашивания.
5. Что представляют собой искусственные маски?
6. Чем засветка отличается от ослепления?
7. Специфика структурного скрытия объекта от радиолокационного наблюдения.
8. Особенности защиты от гидроакустического зашумления.

# Глава 11. Методы противодействия подслушиванию

Методы противодействия подслушиванию направлены, прежде всего, на предотвращение утечки информации в простом акустическом (гидроакустическом, сейсмическом) каналах. Кроме того, для повышения дальности подслушивания применяются составные каналы утечки информации, которые содержат наряду с простыми акустическими также радиоэлектронные (с использованием закладных устройств и вч-навязывания) и оптические (с лазерными средствами) каналы. Поэтому защита информации от подслушивания включает способы и средства блокирования любых каналов, с помощью которых производится утечка акустической информации.

В соответствии с общими методами защиты информации для защиты от подслушивания применяются следующие способы:

1) структурное скрытие, предусматривающее:

- шифрование семантической речевой информации в функциональных каналах связи;
- техническое закрытие электрических и радиосигналов в телефонных каналах связи;
- дезинформирование;

2) энергетическое скрытие путем:

- звукоизоляции акустического сигнала;
- звукопоглощения акустической волны;
- зашумления помещения или твердой среды распространения другими звуками (шумами, помехами), обеспечивающими маскировку акустических сигналов;

3) обнаружение, локализация и изъятие закладных устройств.

Методы предотвращения подслушивания с использованием оптических и радиоэлектронных каналов утечки, входящих в составные каналы, рассматриваются в соответствующих главах.

## 11.1. Структурное скрытие речевой информации в каналах связи

Так как передача речевой информации составляет основу телекоммуникации в человеческом обществе, то ее защита — важней-

шая задача инженерно-технической защиты информации. Речевая информация, передаваемая по каналу связи, содержится в информационных параметрах электрических и радиосигналов. Сигналы распространяются по линиям связи в аналоговом и цифровом виде. В результате несанкционированного перехвата этих сигналов и их модуляции речевая информация может быть добыта злоумышленником.

Для структурного скрытия речевой информации в каналах связи применяют **шифрование** и **техническое закрытие**.

При шифровании аналоговый речевой сигнал с выхода микрофона преобразуется с помощью аналогово-цифрового преобразователя в цифровой сигнал. При аналого-цифровом преобразовании амплитуда сигнала измеряется через равные промежутки времени, называемые шагом дискретизации. Для того чтобы цифровой речевой сигнал имел качество не хуже переданного по телефонному каналу в аналоговой форме, шаг дискретизации в соответствии с теоремой Котельникова не должен превышать 160 мкс, а количество уровней квантования амплитуды речевого сигнала — не менее 128. В этом случае один отсчет амплитуды кодируется 7 битами. Такой вид модуляции сигнала называется импульсно-кодовой комбинацией (ИКМ) и требует скорости передачи 48–64 кбит/с, существенно превышающей пропускную способность стандартного телефонного канала связи. С целью снижения необходимой скорости разработаны различные методы сжатия речевого сообщения. Методы сжатия используют избыточность речевого сигнала или допускают снижение качества речи за счет показателей, несущественных для семантики сообщения. Например, широко применяемый метод дельта-модуляции (ДМ), который предусматривает передачу не абсолютных значений оцифрованных амплитуд исходного речевого сигнала, а величины изменения (дельты) амплитуды при каждом шаге квантования, позволяет снизить скорость передачи до 20–24 кбит/с. Еще меньшая скорость передачи (8–12 кбит/с), но со снижением качества речи, требуется при передаче клипированной речи, которая представляет собой ограниченный по амплитуде дискретный речевой сигнал. Шифрование речевой информации в цифровой форме производится известными методами (заме-

ной, перестановками, аналитическими преобразованиями, гаммированием и др.).

Гарантированное засекречивание сообщений обеспечивается при использовании стандартизованных алгоритмов типа DES в США и ГОСТ 28147-89 в России. Алгоритм DES, применяемый в США с 1976 года, обеспечивает суперпозицию шифров, состоящих из 16 последовательных циклов и в каждом из которых сочетаются подстановки и перестановки. Он реализуется программно, обеспечивает скорость передачи 10–200 кБ/с и криптостойкость $10^{17}$ операций при длине ключа 56 бит.

Алгоритм криптографического преобразования, определяемый ГОСТ 28147-89, обладает криптостойкостью, оцениваемой $10^{70}$ операций (длина ключа 256 бит), обеспечивает скорость шифрования 50–70 кБ/с и реализуется в основном аппаратно. С увеличением длины ключа время раскрытия шифртекста резко возрастает. Например, при быстродействии компьютера около $10^{12}$ оп./с это время составляет около 10 ч для ключа длиной 56 бит, для ключа в 64 бита оно повышается до 3,2 месяца, при длине 70 бит — 17,5 лет, а для 75 бит превышает 560 лет.

Хотя развитие связи характеризуется постепенной заменой аналоговой техники на цифровую, менее дорогая аналоговая связь, особенно телефонная проводная, еще длительное время будет одним из основных видов связи. Но стандартный телефонный канал имеет узкую полосу пропускания в 3 кГц, недостаточную для передачи с высоким качеством шифрованного цифрового сигнала.

Скрытие речевого сигнала в узкополосном телефонном канале осуществляется методами **технического** или **аналогового закрытия**. По названию технических средств, обеспечивающих техническое закрытие, эти методы называются также **скремблированием** (перемешиванием). Техническое закрытие (скремблирование) отличается от криптографического тем, что при шифровании происходит скрытие речевого сообщения в символьной форме, а при техническом закрытии — скрытие речевого сигнала без преобразования его в цифровую форму. При техническом закрытии изменяются признаки (характеристики) исходного речевого сигнала таким образом, что он становится похож на шум, но занимает ту

же частотную полосу. Это позволяет передавать скремблированные сигналы по обычным стандартным телефонным каналам связи. Классификация методов технического закрытия приведена на рис. 11.1.

По виду преобразования сигнала различают частотные и временные методы технического закрытия, а по режиму закрытия — статическое и динамическое. Частотные методы скремблирования, реализуемые на элементах аналоговой техники, появились раньше временных методов, которые выполняются существенно проще на элементах дискретной техники. В настоящее время в связи с прогрессом в микроминиатюризации дискретной техники оба метода используют дискретную элементную базу.

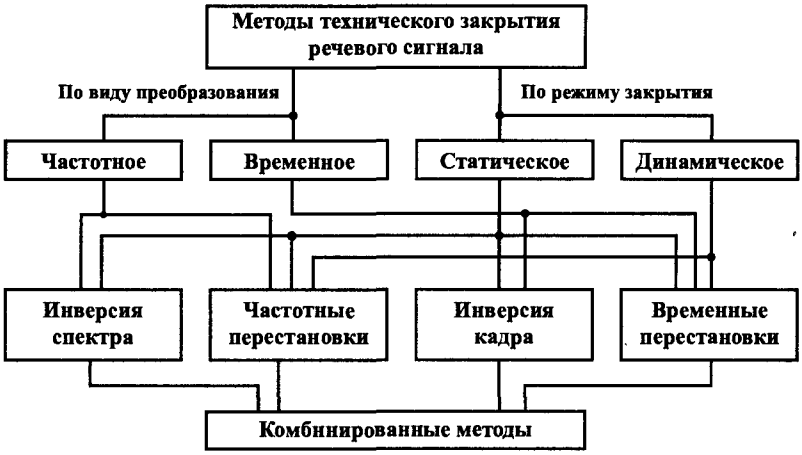
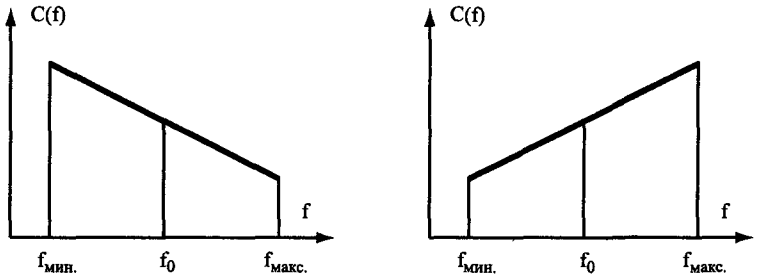



*Рис. 11.1.* Классификация методов технического закрытия

Наиболее простыми способами являются **частотная** и **временная инверсии**. В скремблере, осуществляющем инверсию спектра и называемом также **маскиратором**, осуществляется поворот спектра речевого сигнала вокруг некоторой центральной частоты $f_0$ (рис. 11.2).

Речевой сигнал с инверсным спектром передается по телефонному каналу связи. На приемной стороне осуществляется обратная

процедура, восстанавливающая исходный спектр речевого сигнала. Неподготовленный слушатель воспринимает инверсную речь как нечленораздельный набор звуков. Однако после некоторой тренировки слуховой анализатор человека способен восстанавливать преобразованную речь и воспринимать на слух семантику речевого сообщения. Легко определяемый алгоритм преобразования спектра усложняют в коммутируемом маскираторе путем передачи части речевого сигнала без инверсии и с инверсией. Низкая стоимость маскираторов и их способность устойчиво работать в каналах связи плохого качества способствуют их достаточно широкому применению.

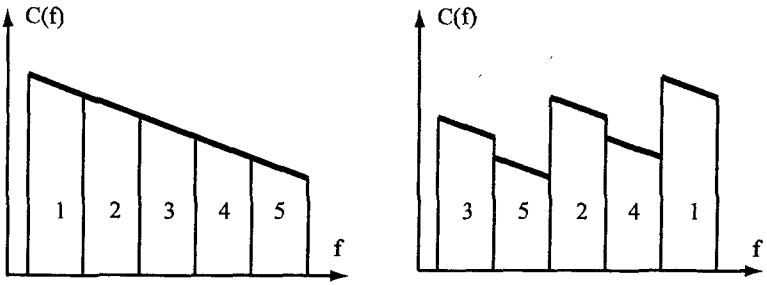



*а*) Исходный сигнал *б*) Преобразованный сигнал

*Рис. 11.2.* Принципы инверсии частотного спектра речевого сигнала

В скремблере, выполняющем **частотные перестановки**, спектр исходного речевого сигнала разделяется на несколько частотных полос равной или неравной ширины (в современных моделях число полос может достигать 10–15) и производится их перемешивание по некоторому алгоритму — ключу (рис. 11.3). При приеме спектр сигнала восстанавливается в результате обратных процедур.

Изменение ключа в ходе сеанса связи в скремблерах с динамическим закрытием позволяет повысить степень закрытия, но при этом требуется передача на приемную сторону сигналов синхронизации, соответствующих моментам смены ключа.



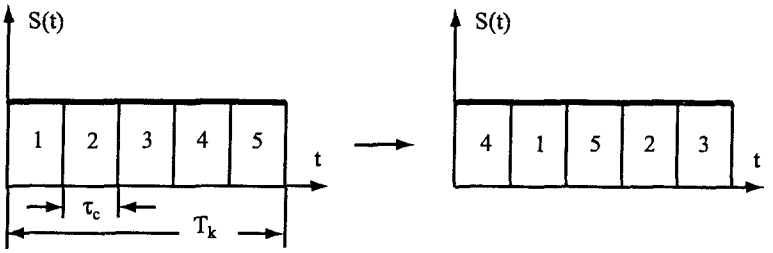

*а*) Исходный сигнал *б*) Преобразованный сигнал

*Рис. 11.3.* Принципы частотной перестановки

Другие виды преобразования носителя речевой информации реализуют **временные** методы технического закрытия с более высоким уровнем защиты информации. **Инверсия кадра** обеспечивается путем предварительного запоминания в памяти передающего скремблера отрезка речевого сообщения (кадра) длительностью $T_k$ и считывание его (с передачей в телефонную линию) с конца кадра — инверсно. При приеме кадр речевого сообщения запоминается и считывается с устройства памяти в обратном порядке, что обеспечивает восстановление исходного сообщения. Для достижения неразборчивости речи необходимо, чтобы продолжительность кадра была не менее 250 мс. В этом случае суммарная продолжительность запоминания и инверсной передачи кадра составляет примерно 500 мс, что может создать заметные задержки сигнала при телефонном разговоре.

В процессе технического закрытия с **временной перестановкой** кадр речевого сообщения делится на отрезки (сегменты) длительностью $\tau_c$ каждый. Последовательность передачи в линию сегментов определяется (правилом) ключом, который должен быть известен приемной стороне (рис. 11.4).

Изменением ключа в ходе сеанса связи в скремблерах с динамическим закрытием можно существенно повысить уровень защиты речевой информации. Остаточная разборчивость зависит от длительности кадра и с увеличением последнего уменьшается.




*а*) Исходное сообщение *б*) Преобразованное сообщение

*Рис. 11.4.* Принципы временной перестановки

Вследствие накопления информации в блоке временного преобразования появляется задержка между поступлением исходного речевого сигнала в передающий скремблер и восстановлением его в приемном скремблере. Если эта задержка превышает 1–2 с, то она создает дискомфорт во время разговора по телефону. Поэтому $T_k$ выбирают менее этого предельного времени и делят на 4–16 сегментов.

Временные инверсия и перестановки технически реализуются путем преобразования исходного речевого сигнала в цифровую форму с помощью аналогово-цифрового преобразователя, цифровой обработки и обратного преобразования закрытого цифрового сигнала в аналоговый, который передается по телефонной линии связи. В приемной части скремблера выполняются с помощью элементов дискретной техники обратные преобразования: восстановление исходного сообщения и преобразование его из цифровой формы в аналоговую.

Используя комбинацию временного и частотного скремблирования, значительно повышают степень закрытия речи. В комбинированном (частотно-временном) скремблере исходное сообщение разделяется на кадры и сегменты, которые запоминаются в памяти скремблера. При формировании передаваемого сообщения производятся временные перестановки сегментов кадра и перестановки полос спектра речевого сигнала каждого сегмента, Если при этом обеспечить динамическое изменение ключа временной и частотной перестановки, то уровень защиты такого комбинированно-

го технического закрытия может не уступать цифровому шифрованию. Однако сложность реализации такого способа и требования к качеству передачи синхроимпульсов между скремблерами телефонных абонентов также высоки.

Основное достоинство методов технического закрытия — простота (по отношению к шифрованию) технической реализации скремблеров и, как следствие, меньшая их стоимость, а также возможность эксплуатации скремблеров практически на любых каналах связи, предназначенных для передачи речевых сообщений. Основной недостаток методов технического закрытия — более низкая стойкость закрытия информации. Кроме того, скремблеры, за исключением простейшего (с частотной инверсией), вносят искажения в восстановленный речевой сигнал. Их появление вызвано тем, что искажаются границы частотных полос и временных сегментов при обратном преобразовании сигнала на приемной стороне, что приводит к некоторому искажению спектра восстановленного речевого сигнала. Нежелательное влияние оказывают и групповые задержки составляющих речевого сигнала. Внесенные техническими средствами искажения приводят к снижению избыточности восстановленного речевого сигнала на (3–5)%.

Однако, несмотря на указанные недостатки, методы временного и частотного скремблирования, а также их различные комбинации позволяют обеспечить защиту информации на тактическом и на приближающемся к стратегическому уровнях защиты. Для технического восстановления речи требуется запись закрытого сообщения на аудиомагнитофон, длительная и трудоемкая работа с использованием дорогостоящей аппаратуры. Техническое закрытие в основном используется в коммерческих каналах связи для защиты конфиденциальной информации.

Передача по узкополосному телефонному каналу речевого сигнала в цифровой форме, позволяющая шифровать речевое сообщение, начала претворяться в жизнь с конца 30-х годов в устройстве, названном **вокодером (кодировщиком голоса)**. Метод передачи речевой информации в вокодере принципиально отличается от иных методов ее передачи. Отличие заключается в том, что в приемном вокодере речевой сигнал синтезируется (восстанавливается)

по медленно меняющимся признакам исходного речевого сигнала. Такая возможность обусловлена тем, что в речевом сигнале наряду с семантической информацией содержится большой объем сопутствующей (сигнальной) информации, характеризующий индивидуальность речи и эмоциональное состояние говорящего человека, который можно существенно уменьшить без изменения смысла речевого сообщения. Конечно, в некоторых случаях для разговаривающего человека важны интонации голоса собеседника, отражающие его подсознательную реакцию на слова. Но в большинстве случаев достаточно обеспечить узнаваемость голоса абонента и понятность его речи. В передающем устройстве вокодера из речевого сигнала выделяются медленно изменяющиеся информационные параметры. Такими параметрами являются:

- частота основного тона акустического сигнала, возникающего при прохождении воздушного потока через голосовые связки говорящего человека;
- моменты произношения локализованных (звонких) и глухих звуков;
- параметры речевого сигнала, зависящие от типа вокодера.

В зависимости от видов параметров речевого сигнала и методов их определения различают фонемные, формантные, полосовые, ортогональные, ЛПК-вокодеры (с линейно-прогнозирующим кодированием). Скорость передачи речевой информации вокодерами составляет 1200–2400 бит/с.

По переданным информационным параметрам синтезируется речь человека в соответствии с электрической моделью его голосового аппарата, указанной на рис. 11.5.

По команде устройства управления (аналога слухового центра мозга) включается источник питания (аналог легкого) и генератор основного тона (звонких звуков) и шума (согласных глухих звуков). Параметры звонких и глухих звуков определяются устройством управления. Управляемый переключатель «тон-шум» подключает к фильтру, формирующему спектр звука, сигналы основного тона или шума. Синтезированный акустический сигнал озвучивается телефоном или громкоговорителем.

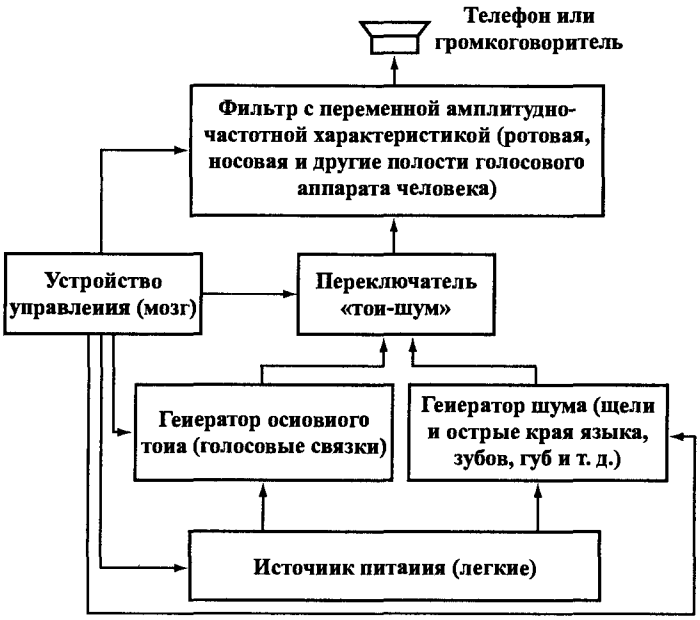



*Рис. 11.5.* Электрическая модель голосового аппарата человека

Основным достоинством систем цифрового шифрования речевого сигнала является высокая надежность закрытия информации, так как перехваченный сигнал представляет из себя случайную цифровую последовательность. Для восстановления из нее исходного сообщения необходимо знать криптосхему шифратора и устройство вокодера.

Недостатком устройств цифрового шифрования речи являются необходимость использования модемов, техническая сложность и относительно большие габариты шифраторов, неустойчивая работа устройств в каналах с большим затуханием сигнала и с высоким уровнем помех.

Сравнительные возможности различных методов закрытия речи указаны на рис. 11.6 [25].

Под **тактическим** (низким или закрытием с временной стойкостью) понимается уровень, обеспечивающий защиту информации от подслушивания посторонними лицами в течение от минут


*Рис. 11.6.* Уровни защиты различных методов закрытия речевой информации

до нескольких дней. Для дешифрования перехваченных сообщений **со стратегическим** (высоким, с гарантированной стойкостью) уровнем защиты информации высококвалифицированному, технически хорошо оснащенному специалисту потребуется от нескольких месяцев до многих лет.

## 11.2. Энергетическое скрытие акустического сигнала

Энергетическое скрытие акустических сигналов в соответствии с рассмотренными методами защиты информации обеспечивается путем применения способов и средств, уменьшающих энергию носителя на входе акустического приемника злоумышленника или увеличивающих энергию помех.

Простейшим способом является **уменьшение громкости** речи во время разговора на конфиденциальные темы. Однако это возможно, если количество собеседников мало, а уровень шумов невелик. Громкость акустического сигнала уменьшают путем **звукоизоляции, звукопоглощения** и **глушения звука**. Для повышения уровня акустических помех применяют активные средства — **генераторы акустических помех**.

**Звукоизоляция** обеспечивает локализацию акустических сигналов в замкнутом пространстве внутри контролируемых зон. Основное требование к ней — за пределами этой зоны соотношение сигнал/помеха не должно превышать максимально-допустимые значения, исключающие добывание информации злоумышленниками. Звукоизоляция достигается за счет отражения и поглощения акустической волны.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Отражательная способность поверхности преграды зависит от плотности ее материала и скорости распространения звука в ней. Отражение акустической волны, распространяющейся в воздухе, от твердой поверхности можно представить себе как результат соударения молекул воздуха в виде движущихся со скоростью $V_в$ упругих шариков массой m с неподвижными шарами большей массы M, соответствующих молекулам поверхности твердой среды. После соударения более массивный шар приобретает скорость $V_c = V_в \frac{m}{M + m}$. Когда $M >> m$, то скорость массивного шара близка к нулю. В этом случае почти вся кинетическая энергия акустической волны преобразуется в потенциальную энергию упругой деформации неподвижных шаров. При восстановлении формы деформированные шары сообщат ударяющим шарам близкую к первоначальной скорость, но в обратном направлении. Возникнет отраженная акустическая волна.

Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и акустических свойств материала. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны. Характер этого поглощения определяется соотношением частот падающей акустической волны и спектральных характеристик средства звукоизоляции. В области резонансных частот (до 25–45 Гц) средств звукоизоляции ослабление зависит в основном от внутреннего трения в звукоизолирующем материале, на более высоких частотах — от его поверхностной плотности, измеряемой в кг на 1 $м^2$ поверхности. С учетом действую-

щих норм на звукоизоляцию в помещении поверхностная масса основных ограждающих конструкций должна составлять не менее 250–300 кг.

В соответствии с формулой Рэлея коэффициент проникновения акустической волны в материал преграды $\chi_{пр} = 4\frac{v_в\rho_в}{v_п\rho_п}/\left(\frac{v_в\rho_в}{v_п\rho_п}+1\right)^2$, где $v_в$ и $v_п$ — скорость распространения акустической волны в воздухе и материале преграды, а $\rho_в$ и $\rho_п$ — удельная плотность воздуха и материала преграды. Произведение $v_в\rho_в$ и $v_п\rho_п$ называется **акустическим сопротивлением воздуха и материала преграды**. Когда акустическое сопротивление материала преграды существенно выше акустического сопротивления воздуха, то $\chi_{пр} \approx 4v_в\rho_в/v_п\rho_п$. Как следует из этой приближенной формулы, чем больше отличаются акустические сопротивления сред, тем больше коэффициент отражения акустической волны от границы их раздела. Например, коэффициент отражения акустической среды от гладкой бетонной стены составляет около 0,99.

Если обозначить интенсивность падающей на поверхность преграды акустической волны как $I_{пад}$, отраженной как $I_{отр}$, поглощенной в прегаде как $I_{погл}$, а прошедшей через преграду как $I_{пр}$, то в соответствии с законом сохранения энергии при встрече акустической продольной волны с преградой выполняется условие: $I_{отр} + I_{погл} + I_{прош} = I_{пад}$ (рис. 11.7).

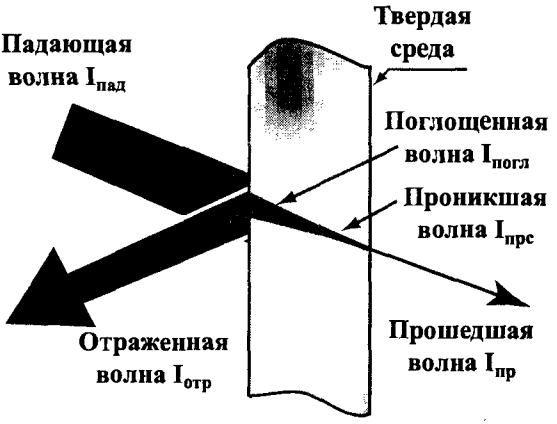



*Рис. 11.7.* Виды акустических волн

Разделив обе части равенства на $I_{пад}$, получим:

$$\beta + \alpha + \gamma = 1,$$

где $\beta = I_{отр}/I_{пад}$ — коэффициент отражения падающей акустической волны поверхностью преграды; $\alpha = I_{погл}/I_{пад}$ — коэффициент поглощения падающей акустической волны материалом преграды; $\gamma = I_{прош}/I_{пад}$ — коэффициент пропускания преградой падающей акустической волны.

Коэффициент $\gamma$ косвенно характеризует звукоизоляцию преграды. Чем меньше коэффициент пропускания преградой акустической волны, тем выше ее звукоизоляция. Количественно звукоизоляция оценивается в логарифмическом масштабе обратной величиной, равной $Q_{зв} = 20\lg(I_{пад}/I_{пр})$, и измеряется в дБ.

Так как $\gamma = 1 - \alpha - \beta$, то звукоизоляция речевого сигнала в выделенном помещении повышается за счет увеличения как $\alpha$, так и $\beta$. Однако при большом значении коэффициента $\alpha$ и малом $\beta$ уменьшается слышимость речи в местах помещения, удаленных от ее источника. При обратном соотношении значений этих коэффициентов может существенно увеличиться время реверберации, возникнет гулкость помещения и ухудшится понятность речи. Рациональное соотношение между этими коэффициентами обеспечивает время реверберации, близкое к оптимальному. Оно достигается как за счет количества звукопоглощающих материалов с определенными характеристиками в помещении, так и их распределения на ограждающих конструкциях с учетом конфигурации и геометрических размеров помещения.

Плоский слой звукопоглощающего материала облицовок устанавливается на жестком основании, которое крепится непосредственно или с воздушным промежутком на поверхности ограждения, к потолку или стенам. Для дополнительного звукопоглощения и уменьшения числа переотражений от ограждений с целью снижения времени реверберации используются **штучные звукопоглотители**. Они представляют собой одно- или многослойные объемные звукопоглощающие конструкции (в виде куба, параллелепипеда, конуса), подвешиваемые к потолку помещения. Размеры граней штучных звукопоглотителей составляют 40–400 см.

Каналы вентиляции и систем кондиционирования также способствуют утечке информации из помещения. Передача звука че-

рез вентиляционный канал происходит по воздуху, находящемуся в полости канала, и по элементам его конструкции. Наиболее эффективной мерой предотвращения утечки информации через воздухопроводы является глушение звука.

**Глушение звука** достигается путем интенсивного поглощения энергии акустической волны при распространении ее в специальной конструкции, называемой **глушителем**. Например, в момент выхода газов из цилиндра двигателя автомобиля в выходном коллекторе создается акустическая волна большой интенсивности. Она направляется по трубе в глушитель, в котором, проходя через многочисленные преграды, теряет энергию и выходит из выхлопной трубы с энергией, сравнимой с энергией акустического фона. При прогорании глушителя или его съеме, что делают иногда на спортивных автомобилях для повышения их мощности, работа двигателя сопровождается интенсивным шумом.

Громкость звука, воспринимаемого человеком, зависит не только от его собственной интенсивности, но и от других звуков, действующих одновременно на барабанную перепонку уха. В силу психофизиологических особенностей восприятия звука человеком интенсивность маскирующих звуков обладает асимметричностью. Она проявляется в том, что маскирующий звук оказывает относительно небольшое влияние на тоны маскируемого звука ниже его собственной частоты, но сильно затрудняет восприятие более высоких звуков. Поэтому для маскировки акустических сигналов эффективны низкочастотные **акустические шумовые сигналы**. Причем речеподобными помехами обеспечивается более эффективное зашумление, чем «белым» шумом. Это объясняется большей восприимчивостью слухового анализатора к речеподобным звукам, чем к акустическому шуму с равномерным спектром.

Следует отметить, что акустическое зашумление помещения обеспечивает эффективную защиту информации в нем, если акустический генератор расположен к акустическому приемнику злоумышленника ближе, чем источник информации. Например, когда подслушивание возможно через дверь или открытое окно, то акустический генератор целесообразно разместить возле двери или на подоконнике окна. Если неизвестно местонахождение акустического приемника злоумышленника, например закладного устройства, то размещение акустического генератора между говорящи-

ми людьми, как рекомендуют некоторые фирмы, не гарантирует надежную защиту информации. Кроме того, повышение уровня шума вынуждает собеседников к более громкой речи, что создает дискомфорт и снижает эффект от зашумления.

Снижение дискомфорта, вызванного акустическими шумами в помещении, достигается использованием специальных переговорных телефонов и акустических приемников, в которых устраняется акустический шум.

Более эффективным и активным универсальным способом защиты информации, передаваемым структурным звуком, является **вибрационное зашумление**. Шум в звуковом диапазоне в твердых телах создают пьезокерамические вибраторы акустического генератора, прикрепляемые (приклеиваемые) к поверхности зашумляемого ограждения (окна, стены, потолка и др.) или твердотельного звукопровода (батареи отопления, трубы и др.). Так как уровень структурного шума, создаваемого генератором, выше уровня речевого сигнала в твердых телах, но ниже уровня слышимости, то вибрационное зашумление целесообразно применять во всех случаях, когда существует возможность утечки с помощью структурного звука.

Пассивное энергетическое скрытие акустической информации от подслушивания лазерным микрофоном заключается в ослаблении энергии акустической волны, воздействующей на оконное стекло. Оно достигается использованием штор и жалюзей, а также двойных оконных рам. Активные способы энергетического скрытия акустической информации предусматривают применение генераторов шумов в акустическом диапазоне, датчики которых приклеиваются к стеклу и вызывают его колебание по случайному закону с амплитудой, превышающей амплитуду колебаний стекла от акустической волны.

## 11.3. Обнаружение и подавление закладных устройств

### 11.3.1. Демаскирующие признаки закладных устройств

Обнаружение закладных устройств, так же как и любых других объектов, производится по их демаскирующим признакам. Чем больше демаскирующих признаков в признаковой структуре и чем они информативнее, тем выше вероятность обнаружения объекта. Каждый вид закладных устройств имеет свою признаковую структуру, позволяющую с той или иной вероятностью обнаружить закладку. Распознавание закладки, т. е. определение ее вида, назначения и характеристик, проводится в результате анализа схемотехнических и конструктивных решений. Однако внешний вид закладки и способы ее оперативного применения позволяют приблизительно определить принадлежность злоумышленника к зарубежной разведке, конкуренту или криминальным элементам.

Спецслужбы используют наиболее совершенные средства добывания, как правило, отсутствующие на рынке, и тщательно готовят операцию по установке закладок. Криминальные элементы пользуются средствами, имеющимися на «черном» рынке, и действуют более грубо. Разведка коммерческих структур применяет закладки промышленного или собственного изготовления и тщательно скрывает от конкурента свои намерения получения конфиденциальной информации нелегальными способами.

Наиболее информативные прямые и косвенные признаки закладных устройств приведены в табл. 11.1.

*Таблица 11.1*

| *Вид признака* | *Наименование признака* |
|---|---|
| Видовой | Тонкий провод от миниатюрного микрофона в соседнее помещение, малогабаритный предмет в виде параллелепипеда, цилиндра или иной формы с проводом (антенной), одно или несколько отверстий малого диаметра в кожухе, выключатель на кожухе, свежие царапины на элементах крепления технических средств, несоответствие топологии схемы радиоэлектронного устройства документации или топологии других однотипных образцов, несоответствие рентгеновского изображения конструкции ее назначению |
| Сигнальный | Радио- и ИК-диапазон излучений, электрический сигнал в проводе частотой десятки–сотни кГц и более, АМ и ЧМ несущего колебания речевым сигналом, ширина полосы сигнала — десятки, реже сотни кГц, простые технические методы закрытия радиосигнала, случайные изменения напряжения в телефонной линии, емкости, индуктивности, дополнительные неоднородности в телефонной линии |
| Вещественный | Нелинейность элементов и металлические детали в малогабаритной конструкции, непрозрачность рентгеновским лучам, пустота в твердой среде с неизвестным вложением |

Камуфлированные радиозакладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Некоторые камуфлированные закладные устройства неотличимы от оригиналов при внешнем осмотре. Например, на поверхность закладки-конденсатора наносятся заводские реквизиты — тип, величина емкости, номер серии и т. д. Назначение таких закладок можно выявить путем разборки или просвечивания их рентгеновскими лучами.

Однако следует иметь в виду, что закладки, камуфлированные под малогабаритные предметы, снижают, но не всегда, функциональные возможности этих предметов. Поэтому обнаруженные ограничения функций средств оргтехники, электробытовых устройств и др. могут служить косвенными признаками установки

в них закладных устройств. Например, в шариковой авторучке закладное устройство занимает приблизительно половину ее длины, в результате чего резко укорачивается пишущий стержень и сокращается время нормальной работы ручки. Кроме того, такую ручку нельзя разобрать, например, для замены стержня, так как разбираемые части склеивают. Таким образом, закладные устройства содержат видовые, сигнальные и вещественные демаскирующие признаки, информативность которых позволяет их обнаруживать среди других объектов.

### 11.3.2. Методы обнаружения закладных подслушивающих устройств

В зависимости от демаскирующих признаков закладных устройств методы их поиска можно разделить на 3 группы (рис. 11.8):

- поиск закладных устройств по их видовым признакам;
- поиск закладных устройств по их сигнальным признакам;
- поиск закладных устройств по их вещественным признакам.

Поиск закладных устройств по видовым признакам осуществляется путем визуального осмотра помещения сотрудниками службы безопасности или иными сотрудниками. Визуальный осмотр требует минимальных затрат по сравнению с другими и может производиться периодически как силами службы безопасности, так и секретарем руководителя организации или иного должностного лица.

Сущность поиска закладки путем визуального осмотра состоит в тщательном осмотре помещения, предметов мебели (книжного шкафа и полок, столов, стульев, кресел, дивана, и др.), компьютера, радио- и электробытовых устройств, телефонных аппаратов, устройств громкоговорящей и диспетчерской связи, картин на стенах, портьер и жалюзей, других предметов в помещении, в которых в принципе можно спрятать малогабаритное закладное устройство. Осмотр проводится без разборки рассматриваемого предмета.

В целях обеспечения полноты визуального контроля целесообразно проводить его по определенной схеме, аналогичной схеме осмотра места происшествия криминалистами: от двери по или против часовой стрелки от периферии к центру помещения. Во время осмотра обращается внимание на свежие царапины на обоях, возле

сетевых и телефонных розеток и выключателей освещения, на с нах, винтах корпуса телефонного аппарата, на пылевые следы см щения картины или других предметов, на отрезки проводов и другие следы или непонятные на первый взгляд предметы.

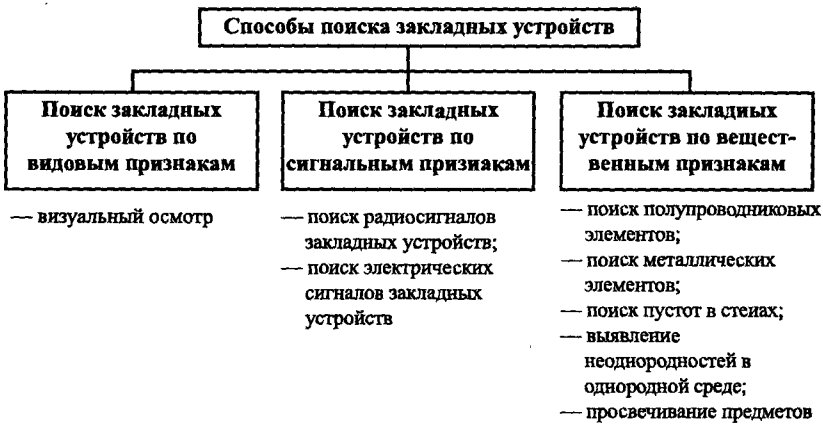



*Рис. 11.8.* Способы поиска закладных устройств

Для визуального осмотра при поиске закладных устройств применяют различное вспомогательное оборудование. Это оборудование, имея невысокую стоимость, позволяет повысить вероятность обнаружения закладки в ходе визуального осмотра помещения. К такому оборудованию относятся фонари, досмотровые зеркала и технические эндоскопы.

Конечно, путем визуального осмотра помещения и предметов интерьера далеко не всегда удается обнаружить скрытно установленные закладные устройства, но периодический осмотр помещения позволяет выявить закладные устройства, установленные в спешке или встроенные в предметы, ранее отсутствующие в помещении. Секретарь, наблюдающий многократно в течение рабочего дня предметы в кабинете, быстрее обнаружит изменения в помещении, чем любой другой сотрудник.

Поиск закладных устройств, вмонтированных в технические средства, производят в ходе специальных исследований путем сравнения топологии схемы исследуемого образца с эталонной, зафиксированной в документации или в топологии образца, в котором заведомо нет закладного устройства. Для обеспечения нераз-

рентгеновского контроля применяются специальные рентгеновские установки, позволяющие наблюдать изображения отдельных слоев микросхем и многослойных печатных плат.

Остальные методы предусматривают поиск закладных устройств дистанционно с использованием различных технических средств, способных обнаруживать сигнальные и вещественные демаскирующие признаки закладных устройств. Так как наиболее распространены радиоизлучающие закладные устройства, то их поиск производится путем обнаружения сигнальных демаскирующих признаков радиоизлучающих закладных устройств.

Наиболее широко применяются следующие методы поиска закладных устройств по их прямым и косвенным сигнальным демаскирующим признакам:

- поиск источников радиоизлучений, мощность которых превышает мощность электромагнитного фона;
- поиск и селекция радиосигналов по частоте с последующей идентификацией их текущей признаковой структуры с эталонной признаковой структурой закладного устройства;
- поиск проводных закладных подслушивающих устройств по косвенным признакам изменений электрических характеристик линий, к которым подключены эти устройства.

Учитывая повсеместное распространение телефонов как средств коммуникаций и особый интерес злоумышленников к подслушиванию телефонных разговоров, при обеспечении защиты информации большое внимание уделяется способам и средствам контроля телефонных линий.

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного сопротивления. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного — в разрыв провода телефонного кабеля, параллельного или индуктивного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и

его коэффициента полезного действия. Наилучшие возможности по выявлению этих отклонений обеспечиваются при опущенной трубке телефонного аппарата. Это обусловлено тем, что в этом состоянии в телефонную линию подается постоянное напряжение 48–60 В (для отечественных телефонных линий) и 25–36 В (для зарубежных АТС). При поднятии трубки в линию поступает от АТС дискретный сигнал, преобразуемый в телефонной трубке в длинный прерывистый тон, а напряжение в линии уменьшается до 12 В, т. е. происходит резкое изменение электрических параметров линии, существенно превышающие изменения из-за закладных устройств.

Для контроля телефонных линий применяются следующие устройства:

- устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;
- измерители характеристик телефонных линий (напряжения, тока, емкостного сопротивления и др.), при отклонении которых от установленных норм формируется сигнал тревоги;
- «кабельные радары», позволяющие измерять неоднородности телефонной линии и определять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.).

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией изменения его значения от номинального, которое фиксируется оператором в режиме настройки вращением регулятора на лицевой панели устройства. Предполагается, что при установке номинального напряжения к телефонной линии подслушивающее устройство не подключено. Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет «микрофонного эффекта»» в элементах телефонного аппарата и высокочастотного навязывания.

Но устройства контроля телефонной сети по изменению напряжения или тока в ней не обеспечивают надежного обнаружения подключаемых параллельно к линии современных средств подслушивания с входным сопротивлением более единиц МОм.

Повышение реальной чувствительности устройств контроля ограничено нестабильностью параметров линии, колебаниями напряжения источников электропитания на АТС, помехами в линии. Для снижения вероятности ложных тревог в более сложных подобных устройствах увеличивают количество измеряемых характеристик линии, предусматривают возможность накопления и статистической обработки результатов измерений в течение достаточно длительного времени как контролируемой линии, так и близко расположенных.

Так как любое физическое подключение к кабелю телефонной линии создает в ней неоднородность, от которой отражается посылаемый в линию сигнал, то по характеру отражения (амплитуде и фазе) и времени запаздывания отраженного сигнала оценивают вид неоднородности и рассчитывают длину участка линии до неоднородности (места подключения).

Разнообразие радиоизлучающих и проводных закладных устройств и способов их применения способствует объединению в автоматизированном комплексе средств, реализующих все способы поиска и обнаружения активных закладных устройств. Более того, в них устанавливаются генераторы прицельной помехи, настраиваемой на частоту закладного устройства и подавляющей их сигналы в свободном пространстве и в проводах кабелей. Такая тенденция обеспечивает снижение суммарной стоимости средств поиска и обнаружения закладных устройств по их сигнальным признакам и оперативность подавления их сигналов в экстремальных ситуациях, например, во время ответственного совещания, когда крайне нежелательно проводить поисковые мероприятия в помещении или зале совещания.

Поиск и обнаружение дистанционно управляемых и пассивных (параметрических) закладных устройств производятся по прямым и косвенным признакам входящих в их состав веществ. Прямыми признаками закладных устройств является наличие в них полупроводниковых и металлических элементов. Косвенные признаки установки закладного устройства в стене или иной твердой среде — наличие в них пустоты.

Так как любое радиоэлектронное закладное устройство содержит полупроводниковый элемент (транзистор, диод), то наиболее информативным признаков не излучающего во время поиска за-

кладного устройства является наличие полупроводниковых элементов в местах, в которых не должно быть радиоэлектронных устройств. Такими местами являются стены, мебель, картины, подвесные потолки и др. Для обнаружения полупроводникового элемента используются нелинейные свойства его вольтамперной характеристики — зависимости тока, протекающего по n–p переходу полупроводника, от величины подводимого к нему напряжению. Вихревые электрические токи через n–p переходы полупроводников возникают при облучении проводника электромагнитным полем. Поле создает антенна передатчика нелинейного локатора, излучающего непрерывные гармонические или импульсные сигналы на частоте f, составляющие для разных локаторов доли и единицы ГГц (400–1000 МГц). В силу нелинейности полупроводника токи в нем имеют форму, отличную от гармонического колебания, и могут быть разложены в ряд Фурье. Вихревые токи создают вторичное электромагнитное поле, содержащее кроме электромагнитной волны на основной частоте f, также волны с частотой 2f, 3f и других частотах спектра вторичного сигнала. В отличие от классического радиолокатора нелинейный локатор имеет приемник, настроенный на частоту 2f, а в некоторых типах дополнительный приемник на частоте 3f. Появление в отраженном сигнале колебаний с частотами 2f и 3f позволяет сделать вывод о наличии в области облучения зондирующей электромагнитной волны элементов с нелинейной вольтамперной характеристикой. Мощность сигнала на второй гармонике в приемной антенне нелинейного локатора определяется по формуле [26]:

$$P_2 = \frac{(P_з G_п)^2 S_{эф}}{(4\pi R^2)^3},$$

где $P_з$ — мощность зондирующего импульса; $G_п$ — коэффициент усиления передающей антенны; $S_{эф}$ — эффективная площадь приемной антенны нелинейного локатора; R — расстояние от локатора до обследуемой поверхности.

На практике достоверность обнаружения полупроводникового элемента снижается в связи с тем, что нелинейными свойствами обладают не только полупроводниковые элементы, но и окислы и места контактов металлических предметов и конструкций поме-

шения и здания: ржавой арматуры железобетонных стен, гвоздей и болтов мебели, даже скрепок для бумаги. Поэтому для обнаружения полупроводников приходится учитывать различия в мощности сигналов на частотах 2f и 3f, отраженных от полупроводников и окисленных металлических конструкций и предметов. Эти различия обусловлены разной формой нелинейных вольтамперных характеристик полупроводниковых и других элементов, что приводит к различиям амплитуд гармоник спектров отраженных сигналов. Для настоящих полупроводников уровень второй гармоники в среднем на 20 дБ превышает уровень 3-й гармоники, для ложных — противоположные соотношения. Но эти отличия не столь существенны для формального однозначного принятия решения о наличии в рассматриваемой области полупроводника, а не иного элемента с нелинейной вольтамперной характеристикой. Поэтому вероятность идентификации полупроводника тем выше, чем более опытным является оператор, проводящий поиск закладного устройства. Для повышения достоверности обнаружения полупроводниковых элементов используется нестабильность вольтамперных характеристик «ложных» полупроводников при механическом воздействии (ударе) по ним. Это связано с тем, что при ударе нарушается контакт между металлическими поверхностями или разрушается пленка окисла, кроме того, при облучении работающего закладного устройства переотраженный им сигнал модулируется по амплитуде первичным информационным сигналом. Предусмотренный в современных нелинейных локаторах режим выделения огибающей переотраженного сигнала и его индикации позволяет обнаруживать и идентифицировать работающие закладные устройства с высокой достоверностью.

Проникающая глубина излучающей волны нелинейного локатора зависит от мощности и частоты излучения. В силу увеличения затухания электромагнитной волны в среде распространения с повышением частоты колебаний уровень мощности переизлученного (отраженного) сигнала тем выше, чем ниже частота локатора. Но для излучений с более низкой частотой ухудшаются возможности локатора по локализации места нахождения нелинейности, так как при приемлемых размерах его антенны расширяется диаграмма направленности антенны локатора.

Очевидно, что чем выше мощность излучения локатора, тем глубже проникает электромагнитная волна и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения оказывает вредное воздействие на оператора. Для обеспечения его безопасности максимальная мощность излучения локатора в непрерывном режиме не превышает 3–5 Вт. При импульсном режиме работы локатора мощность в импульсе достигает 300 Вт при меньшей средней мощности, не превышающей 1,5 Вт.

Очевидно, что после обнаружения закладного устройства его необходимо изъять, разрушить или использовать для дезинформирования. Для изъятия закладного устройства из стены ее приходится долбить. Так как достоверность идентификации закладного устройства в железобетонной стене мала, то разрушения стены во время его поиска могут быть весьма существенны. Для повышения достоверности обнаружения закладных устройств в железобетонных стенах применяют также обнаружители естественных и искусственных пустот, в которых могут быть размещены закладные устройства, а также рентгеновские установки (интерсепторы).

Для обнаружения пустот применяются средства — обнаружители пустот, которые реагируют на отличия диэлектрической проницаемости или теплопроводности воздуха (пустоты) и бетона. Измерительная катушка генератора обнаружителя пустоты локализует место в однородной среде (стене) — пустоту, диэлектрическая проницаемость которого отличается от диэлектрической проницаемости вещества среды. Также будут отличаться температура внутри пустоты и бетона в нагретом солнечными лучами или обогревателем помещении. Границы пустот будут видны на экране тепловизора.

Большие возможности для обнаружения закладных устройств в строительных конструкциях предоставляют методы **подповерхностной локации**. В результате цифровой обработки переотраженных от исследуемой среды сигналов на экране монитора компьютера получают полутоновое изображение твердой среды, например стены на глубине 200–500 мм с разрешением около 2 см [27]. Хотя такое разрешение недостаточно для рассмотрения детальной структуры наблюдаемой неоднородности, оно позволяет отличить

длинные стержни арматуры от локализованного в пространстве закладного устройства.

Для обнаружения закладных устройств в предметах деревянной и мягкой мебели, в кирпичных стенах, в одежде человека используют обнаружители металла — **ручные металлоискатели.** Современные металлоискатели обладают высокой чувствительностью. Некоторые образцы могут обнаруживать кончик швейной иглы длиной в 5 мм на расстоянии нескольких см. Однако если закладное устройство размещено вблизи металлического гвоздя или болта, то достоверность идентификации закладного устройства резко снижается.

Наибольшую достоверность идентификации закладных устройств, скрытно установленных в отдельных предметах, обеспечивают **средства радиационной интроскопии** (рентгеновские установки). Основу этих средств составляют рентгеновские трубки и рентгеновские электронно-оптические преобразователи (РЭОПы), изобретенные в начале 50-х годов Тевисом и Тулом. В настоящее время выпускается третье поколение РЭОПов, отличающееся от предыдущих высоким разрешением — до 3 лин/мм. Средства радиационной интроскопии делят на две группы: флуороскопические и сканирующие, реализующие методы цифровой радиографии. Для поиска закладных устройств применяются пассивные и активные флуороскопические системы. В пассивных изображения внутренней структуры объекта наблюдаются непосредственно на экране РЭОПа, в активных — первичное теневое изображение усиливается или трансформируется дополнительными электронными средствами. Пассивные флуороскопы просты по конструкции и в эксплуатации, недороги, надежны, но создают низкий уровень яркости изображения при достаточно высоких радиационных нагрузках на объект. В современных пассивных флуороскопах экран способен сохранять (запоминать) изображение после выключения высокого напряжения не рентгеновской трубке, что позволяет оператору в безопасных условиях рассматривать изображение без ограничения времени. Активные флуороскопические системы обеспечивают высокую яркость и чувствительность, превышающую в 2 раза чувствительность пассивных систем. Для контроля помещений и отдельных подозрительных объектов наибольшее примене-

ние находят флуороскопы, в которых изображение с экрана РЭОПа передается на дополнительный электронно-оптический преобразователь с помощью стекловолоконного жгута, и рентгенотелевизионные комплексы. В последних первичное изображение проектируется на высокочувствительную телевизионную камеру, а изображение объекта наблюдается на экране монитора, удаленного на безопасное для оператора расстояние от рентгеновской трубки. Современные рентгенотелевизионные комплексы обеспечивают возможность наблюдения с разрешением около 800x600 пикселей объектов размером до 320 × 420 мм за стальной пластиной толщиной до 10 мм.

### 11.3.3. Методы подавления подслушивающих закладных устройств

Обнаружение с той или иной вероятностью закладного устройства является важным, но лишь одним из этапов предотвращения утечки через них информации. Возникает вопрос о дальнейших действиях. Если обнаружено излучение закладного устройства из помещения, где проводится совещание с участием представителей других организаций, то изъятие его в ходе совещания может рассматриваться как крайняя, но не желательная мера, так как она нарушит ход совещания и снизит рейтинг организации, не обеспечившей информационную безопасность до начала совещания. Изъятие закладного устройства не всегда целесообразно даже в условиях поисковых мероприятий, так как важно не только обнаружить его, но и выявить злоумышленника, установившего и использующего это закладное устройство. Кроме того, через него можно передавать злоумышленнику дезинформацию.

Поэтому наряду с изъятием обнаруженных закладных устройств возможны иные различные методы их **функционального** и **физического подавления**. Функциональное подавление приводит к подавлению работоспособности закладного устройства в течение времени воздействия подавляющих сигналов. При физическом подавлении устройство выходит из строя.

Функциональное подавление осуществляется сигналами, проникающими во входные цепи закладного устройства и нарушающими его работоспособность. Функциональное подавление телефонных закладных устройств обеспечивается методами:

- «синфазной» низкочастотной помехи;
- низкочастотной маскирующей помехи;
- высокочастотной маскирующей помехи;
- «ультразвуковой» маскирующей помехи;
- повышения напряжения;
- понижения напряжения;
- компенсации.

В качестве **«синфазной» низкочастотной помехи** в провода телефонной линии подаются низкочастотные (в речевом диапазоне) маскирующие псевдослучайные дискретные сигналы с одинаковыми относительно «земли» амплитудами и фазами. В телефонной трубке такие сигналы компенсируют друг друга. Но в закладном устройстве, подключенном в разрыв или поднесенном при индуктивном снятии информации к одному из проводов телефонной линии, такая помеха маскирует полезный речевой сигнал.

**Низкочастотный сигнал**, подаваемый в телефонную линию при опущенной телефонной трубке, имитирует речевой сигнал, который включает записывающее закладное устройство. В результате этого его память (лента или полупроводниковая память) используют свой ресурс на запись помехового сигнала.

Частота **маскирующей высокочастотной помехи**, подаваемой в телефонную линию, выше верхней частоты стандартного телефонного канала и составляет 6–16 кГц. Сигнал помехи проходит через входные цепи закладного устройства и подавляет полезный сигнал. С целью исключения влияния помехи на сигнал в телефонной трубке между проводами линии включается фильтр низкой частоты с частотой среза около 3400 Гц.

В методе **«ультразвуковой» маскирующей помехи** ее частота выше верхней частоты звукового диапазона. Так как такая помеха не искажает речевой сигнал в линии, то отпадает необходимость в мерах по снижению влияния помехи на качество речи в телефонной линии. Но при этом для обеспечения достаточного уровня помехи, прошедшей через селективные церии закладного устройства, необходимо повышать амплитуду помехового сигнала, подаваемого в линию.

С целью нарушения режимов работы передатчиков закладных устройств (линейности, частоты излучения и др.) в телефонную ли-

нию подают также **дополнительное постоянное напряжение**, повышающее или понижающее номинальное напряжение в линии.

Метод **компенсации** предусматривает подачу в телефонную линию шумового маскирующего сигнала в речевом диапазоне и компенсацию этой помехи на приемной стороне с помощью адаптивного фильтра. На фильтр, включенный в линию до приемного телефонного аппарата, поступают сигнал с помехой из телефонной линии и помеха, подаваемая в линию от генератора помех. В этом случае из сигнала с помехой вычитается помеха, что обеспечивает прослушивание речевого сигнала без помехи.

**Физическое подавление** достигается подачей в телефонную линию импульсных кратковременных сигналов с амплитудой, превышающей напряжение пробоя элементов электрической схемы закладного устройства. Оно выводится из строя и для дальнейшего применения не пригодно. Для гарантированного «выжигания» входных элементов закладного устройства напряжение сигналов физического подавления достигает 1500 В и более. Но при применении метода «выжигания» необходимо строго выполнять требования по отключению от «выжигаемого» участка телефонной линии всех подключенных радиоэлектронных средств и проводов в телефонной коробке или на щите остальных ее участков. Так как закладные устройства могут подключаться к проводам телефонной линии в разрыв одного из них или параллельно, то «выжигание» производится при разомкнутых и замкнутых ее концах.

### 11.3.4. Способы контроля помещений на отсутствие закладных устройств

Для обеспечения безопасности информации в помещении необходим постоянный контроль отсутствия в нем закладных устройств — «чистка» помещения. Целесообразны следующие виды такой «чистки»:

- оперативный визуальный осмотр помещения;
- профилактический периодический контроль с использованием технических средств поиска и локализации закладных устройств;
- разовый контроль помещения перед проведением в нем совещаний по закрытой тематике и после капитального ремонта;

- проверка различных новых предметов, размещаемых в помещении, в том числе представительских подарков, предметов интерьера, радиоэлектронных средств и др.;
- радиомониторинг помещения в течение рабочего времени.

Частота и способы проверки помещений с целью выявления в них закладных устройств зависят от категории помещений и порядка допуска в них посторонних лиц. Наибольшего внимания службы безопасности требуют кабинеты руководителя и его заместителей. В них, с одной стороны, часто ведутся разговоры на закрытые темы, а с другой, эти помещения посещают не только сотрудники организации, но и посторонние лица.

Методика визуального осмотра помещения близка методике осмотра места происшествия, применяемой в криминалистике. Для упорядоченности поиска он проводится от двери по или против часовой стрелки, от периферии к центру помещения. Осматриваются все места, в которых можно установить закладное устройство — щели в строительных конструкциях, полости в навесных потолках, полах и между ребрами батарей отопления, декоративные экраны люстр в местах крепления их к потолку, внутренние поверхности столешниц, стульев и подоконников, щели между книгами и папки с торцевыми отверстиями в шкафу, углубления в мягкой мебели и т. д. При этом обращается внимание на косвенные признаки: свежие царапины на поверхности стен или винтов, локальные участки без пыли, следы подкраски или клея, отставшие от стены участки обоев и их неровности и др.

Для осмотра плохо освещаемых мест применяют фонари. Могут использоваться малогабаритные бытовые фонари, но более удобными являются фонари с улучшенными световыми характеристиками.

Досмотровые зеркала применяются для осмотра труднодоступных мест (мебельных ниш, вентиляционных отверстий, под шкафом, диваном и т. д.). Досмотровые комплекты зеркал включают в себя сменные зеркала различных размеров и конфигурации, телескопическую штангу из колен различной длины и фонарь подсветки.

Для поиска малогабаритных закладок в местах, не просматриваемых с помощью зеркал, можно применять волоконно-оптичес-

кие технические эндоскопы, которые используются для скрытного наблюдения.

Эффективность визуального осмотра повышается при контроле труднодоступных мест с помощью индикаторов поля. Для обеспечения излучения радиозакладки с акустоавтоматом во время проверки необходимо включить радиоприемник, телевизор или громко разговаривать.

Визуальный оперативный осмотр кабинета руководителя организации перед началом или после завершения рабочего дня целесообразно поручить его секретарю, так как он (она) может выявить наиболее быстро новые предметы, появившиеся в кабинете, вплоть до появления новой авторучки на столе. Если проверка проводится вечером, то кабинет должен быть закрыт на ночь, а запасные ключи находиться под наблюдением охраны.

Периодический контроль предусматривает углубленную проверку помещения на наличие в нем всех видов закладок. По решаемым задачам периодический контроль должен обеспечивать обнаружение и локализацию закладных устройств, которые не могут быть выявлены во время визуального осмотра. К таким закладкам относятся камуфлированные и малогабаритные некамуфлированные закладки, в том числе закладки, передающие сигналы по проводам. Периодичность такой чистки устанавливает руководитель исходя из ценности защищаемой информации, которая зависит как от вида деятельности, так и этапа работы. В типовом варианте периодический контроль может проводиться несколько раз в месяц, а также после каждого ремонта с привлечением посторонних лиц, за работой которых трудно организовать постоянное наблюдение. Набор технических средств, используемых при таком контроле, определяется возможностью организации по их приобретению.

Одной из важнейших задач службы безопасности при подготовке к ответственному совещанию является проверка помещения, в котором оно должно проводиться. Необходимость такой проверки вызвана потенциальной возможностью определения конкурентом или злоумышленником времени и тематики совещания и проведения ими операции по установке в комнате совещания закладного устройства, в том числе дистанционно управляемого.

Глубина «чистки» комнаты совещания зависит от характера использования этого помещения в процессе функционирования

организации. Если организация выделяет специальное помещение для проведения совещаний, которое постоянно закрыто на ключ, опечатано печатью ответственного лица, сдается ежесуточно под охрану с соответствующей записью в журнале, то контроль помещения перед совещанием проводится путем визуального осмотра с использованием средств анализа излучений. Если совещание проводится в служебном помещении (кабинете руководителя или его заместителей, в рабочих комнатах сотрудников), то объем проверок соответствует объему периодической «чистки».

Кроме того, нельзя исключить возможность проноса закладки одним из участников совещания. Поэтому эфир возле выделенного помещения целесообразно контролировать и в ходе совещания с помощью автоматизированных комплексов радиомониторинга.

Проведение капитального ремонта помещения связано с угрозой установки в конструктивных или специально созданных пустотах в стенах (для проводов скрытой электропроводки, выключателей и розеток электропитания, вывода проводов для подключения люстры и др.). Постоянно контролировать работников, проводящих ремонт, практически невозможно. Поэтому после капитального ремонта необходимо провести тщательный технический контроль пустого (до размещения мебели и приборов) помещения на отсутствие в нем закладных устройств. Целесообразно мебель и приборы, находящиеся в кабинете, на время ремонта вынести в другое закрываемое и опечатываемое помещение. Если мебель и приборы оставлены в ремонтируемом помещении или вынесены в незакрываемое помещение или в коридор, то проверяется каждый предмет.

Достоверное обнаружение закладок возможно при комплексном применении аппаратуры, выявляющей прямые и косвенные демаскирующие признаки: радиоизлучения, пустоты в стене, металлические и нелинейные элементы. Учитывая высокую стоимость набора такой аппаратуры и сравнительно малую частоту проведения подобного ремонта, для проверки помещения после ремонта целесообразно привлекать специализированные организации.

Обнаруженные закладные устройства изымаются или оставляются на месте для передачи дезинформации. Если изъятие выявленной закладки связано с необходимостью проведения достаточно серьезных строительных работ, то закладки, подключенные

к телефонной линии или цепям электропитания, дешевле «сжечь» высоковольтными импульсами, отсоединив от проверяемой линии все радиоэлектронные средства. Кроме того, провода телефонной линии необходимо отсоединить от распределительной коробки.

Распознавание обнаруженных предметов, а также проверку представительских и других подарков или изделий, приобретаемых по предварительному заказу или с доставкой к месту эксплуатации фирмой посредником, проводится:

- путем механической разборки, если таковая допускается по условиям эксплуатации или не предполагается дальнейшее использование обнаруженного предмета;
- просвечиванием рентгеновскими лучами неразбираемых предметов;
- облучением полем нелинейного локатора предметов, которые по своему прямому функциональному назначению не могут содержать полупроводниковые элементы;
- проведением специальных исследований радиоэлектронной аппаратуры, прежде всего ПЭВМ.

Распознать обнаруженный предмет непонятного по внешнему виду назначения, а не просто его выбросить, важно потому, что факт обнаружения закладки представляет ценную информацию об активных действиях злоумышленника и перехода угроз безопасности информации из состояния потенциальных в состояние реальных.

Различного рода подарки исследуются без нарушения их товарного вида, что возможно путем выявления излучений, дистанционного обнаружения полупроводниковых элементов или просвечивания подарка.

Специальные исследования могут проводиться специалистами при наличии соответствующей аппаратуры. Если не удается выявить закладку по излучаемому ею сигналу, то производится неразрушающая разборка исследуемого средства и анализ каждого из его узлов. Внешними признаками наличия закладки могут быть:

- отличия в технологии монтажа одной из деталей;
- различия в составе и размещении деталей исследуемого узла и идентичного узла другого проверенного средства.

Так как производство современной радиоэлектронной и вычислительной техники основывается на высоких технологиях, требо-

ания которых трудно выполнить на неспециализированном предприятии, то нарушения технологии могут быть выявлены специалистами в процессе внешнего осмотра. Например, установка на печатной плате средства закладки в виде микросхемы или камуфлированной детали потребует изменения топологии или монтажа платы, восстановления ее защитного покрытия, что трудно сделать без появления заметной границы слоя лака, разрушенного при пайке.

В случае отсутствия заметных нарушений технологии монтажа надежное выявление посторонних элементов обеспечивает сравнение исследуемого узла или блока с эталоном. В качестве эталона применяют аналогичные узлы других изделий, например соответствующей платы средства такого же типа. Этот метод связан с дополнительными затратами на приобретение идентичных средств по другим торговым каналам. Поэтому целесообразно при оснащении организации техникой приобретать однотипные средства у разных продавцов с последующим их сравнением. Наиболее трудоемким представляется процесс выявления закладок на основе технической документации исследуемого средства, получение которой может представлять достаточно сложную задачу.

Разнообразие технических средств обнаружения и локализации закладных устройств ставит перед службой безопасности организации проблему их выбора при покупке и эффективной эксплуатации.

Выбор рационального состава средств для «чистки» помещений определяется:

- ценностью защищаемой информации в выделенных помещениях;
- количеством выделенных помещений;
- периодичностью проведения совещаний и других мероприятий с циркуляцией защищаемой информации;
- финансовым состоянием организации.

Возможно большое количество вариантов набора средств, приобретаемых организацией для «чистки» помещения. Рациональный выбор предусматривает такой состав средств, приобретение которых окупается в течение определенного времени (например, до 5 лет) по отношению к затратам на «чистку» помещений с использованием арендованных средств или привлечения специализированных организаций.

## 11.4. Методы предотвращения несанкционированной записи речевой информации на диктофон

Необходимость предотвращения скрытой записи речевой информации на диктофон возникает во время конфиденциального разговора должностного лица организации с посетителем или во время совещания по закрытой тематике. Диктофон может размещаться на теле злоумышленника или в его носимых личных вещах.

Для предотвращения несанкционированной (скрытой) записи речевой информации разговора необходимо, прежде всего, с достаточной достоверностью обнаружить работающий лентопротяжный или цифровой диктофон. После обнаружения диктофона и информирования об этом должностного лица, чей разговор подслушивается, возможны следующие меры обеспечения безопасности речевой информации:

- прекращение разговора или совещания;
- исключение из разговора конфиденциальных вопросов, способных нанести должностному лицу или его организации ущерб, или введение в разговор дезинформации;
- изъятие диктофона у его владельца или стирание записанной на нем информации;
- дистанционное скрытное воздействие электромагнитным полем на работающий диктофон, приводящее к нарушение работы диктофона.

Обнаружение работающих диктофонов представляет сложную задачу, так как производители диктофонов для скрытой записи принимают эффективные меры по исключению или снижению информативности демаскирующих признаков: обеспечивается бесшумность работы лентопротяжного механизма, отсутствуют генераторы подмагничивания и стирания, экранируются головки и корпус и т. д. Цифровые диктофоны не имеют лентопротяжного механизма.

Диктофон, содержащий металлический экран или металлические детали, может быть обнаружен стационарным металлодетектором, встроенным в раму двери кабинета или помещения для совещания, или ручным металлодетектором по договоренности с

частниками совещания. Обыск посетителей с целью обнаружения оружия и диктофонов применяется в исключительных случаях, так как он противоречит деловой этике.

В кинематических диктофонах с записью на магнитной ленте или проволоке наибольшую информативность имеет низкочастотное пульсирующее (переменное) магнитное поле работающего электродвигателя. Спектр этого поля шириной 50–400 Гц содержит гармоники, кратные частоте вращения ротора двигателя. Поле двигателя слабо экранируется тонким корпусом диктофона, но обнаружить его можно лишь на небольшом расстоянии. Задача усложняется из-за наличия в помещении разнообразных низкочастотных полей, создаваемых цепями электропитания, телефонными и другими линиями, многочисленными электро- и радиоприборами, компьютерами, транспортом и т. д., а также из-за неравномерности распределения напряженности электромагнитных полей в помещении. Идентификация работающего диктофона производится путем выявления и анализа изменений параметров полей, измеренных в месте размещения посетителя (участника переговоров или совещания). Путем накопления изменений удается выделить регулярное поле двигателя диктофона на фоне даже более мощных случайных полей других источников. В бескинематических (цифровых) диктофонах задача обнаружения решается путем приема слабых радиосигналов, излучаемых генераторами тактовой частоты устройств памяти диктофонов.

Для исключения записи речи на диктофоны создано большое количество типов активных средств нарушения их работы. Принципы работы этих средств основаны на изменении под действием наводок излучаемого ими электромагнитного поля режимов работы входных каскадов усилителя записи диктофона, в результате чего резко ухудшается разборчивость записываемой речи и становится невозможным ее понимание при воспроизведении.

Мобильное средство подавления, вмонтированное в портфеле типа «дипломат», устанавливается возле руководителя под видом его личного портфеля и ориентируется таким образом, чтобы стул или кресло посетителя попали в зону подавления. Перед началом разговора руководитель или сотрудник СБ незаметно включает средство подавления, после его окончания — выключает.

## 11.5. Методы подавления опасных сигналов акустоэлектрических преобразователей

Степень подавления опасных сигналов, создаваемых случайными акустоэлектрическими преобразователями радиоэлектронных средств и электрических приборов, должна соответствовать следующим требованиям:

а) Опасные сигналы, которые могут содержать конфиденциальную информацию, должны быть ослаблены до уровня, исключающего съем с них информации на границе контролируемой зоны. Учитывая, что чувствительность современных приемников составляет доли мкВ, уровень опасных сигналов на входе приемника, расположенного на границе контролируемой зоны, не должен превышать эти значения. Если уровни опасных сигналов на выходе создающих их устройств, например акустоэлектрических преобразователей, составляют единицы и десятки мВ, то средства защиты должны обеспечить ослабление амплитуд опасных сигналов на 80–100 дБ.

б) Средства защиты не должны вносить заметных искажений в работу функциональных устройств, используемых сотрудниками организации, и не усложнять процесс пользования ими.

Поскольку опасные сигналы являются побочным продуктом работы различных радиоэлектронных средств и возникают случайным образом, а к их источникам, как правило, отсутствует прямой доступ (без нарушения конструкции), то возможности применения способов технического закрытия или шифрования речи в этих электромагнитных каналах утечки отсутствуют. Основной способ защиты информации в них — энергетическое скрытие.

Способы подавления опасных электрических сигналов, распространяющихся из контролируемой зоны по кабелям (электрическим проводам), могут быть **пассивными** и **активными**. Первые обеспечивают уменьшение уровня опасных сигналов, вторые — повышение уровня помех.

Для подавления опасных сигналов их необходимо предварительно обнаружить и выделить среди других сигналов: полезных и шумов. Идентификация опасных сигналов, как любых других объектов, производится путем сравнения их текущих структур с эталонными. Демаскирующими признаками опасных сиг-


*Рис. 11.9.* Классификация способов подавления опасных сигналов акустоэлектрических преобразователей

налов, используемыми для их подавления, являются частота, амплитуда и местонахождение по отношению к полезному сигналу. Классификация этих способов представлена на рис. 11.9.

**Отключение устройств** с акустоэлектрическими преобразователями, создающими опасные сигналы, является наиболее простым и эффективным способом защиты информации. Необходимо отключать в помещении, в котором ведутся конфиденциальные разговоры, все радиоэлектронные средства и электрические приборы, без которых можно обойтись.

**Фильтрация опасных сигналов** эффективна, если частоты опасных сигналов существенно отличаются от частот полезных сигналов. Например, частота полезного сигнала — сигнала вызова 25 Гц существенно меньше нижней частоты стандартного телефонного канала 300 Гц или частота импульсов управления вторичными часами единого времени частоты (1 импульс в минуту) — нижней частоты звукового диапазона. Фильтры низкой частоты с частотой среза выше звукового диапазона обеспечивают защиту информации в телефонных аппаратах от высокочастотного навязывания, не пропуская к ним высокочастотные электрические сигналы от генератора, подключенного злоумышленником к соответству-

ющей телефонной линии. Полезные сигналы в речевом диапазоне частот проходят через фильтр без заметного ослабления.

Если частоты полезного и опасного сигналов перекрываются, но имеют существенно отличающуюся амплитуду, то применяют метод ограничения малых амплитуд. Для **ограничения опасных сигналов** используются нелинейные свойства полупроводниковых элементов (диодов, транзисторов, динисторов, тиристоров), которые имеют для сигналов малой амплитуды (доли мВ) сопротивление, превышающее в десятки и сотни тысяч раз сопротивление сигналам большой амплитуды (десятки В).

Последний из рассматриваемых способов защиты информации применяется, когда единственным признаком отличия опасных сигналов от полезных является направление их распространения. Например, полезные сигналы, подаваемые на громкоговоритель оповещения, и возникающие в нем опасные сигналы имеют близкую по величине амплитуду и одинаковый диапазон частот. Поэтому рассмотренные способы подавления опасных сигналов для него не приемлемы. Задача решается с помощью **буферного устройства**, включаемого между громкоговорителем и проводами линии трансляции. Буферное устройство в виде нескольких последовательно соединенных эмиттерных повторителей пропускает полезный сигнал от внешнего устройства практически без ослабления, а опасные сигналы от громкоговорителя подавляет.

**Активные способы защиты** от опасных сигналов предусматривают генерирование помех в радиодиапазоне для пространственного зашумления, в звуковом и ультразвуковом — для линейного зашумления.

### Вопросы для самопроверки

1. Цель технического закрытия речевой информации в телефонных каналах.
2. Чем отличаются частотные перестановки от временных перестановок?
3. Искажения, возникающие при частотных и временных перестановках.
4. Параметры речевого сигнала, используемые в вокодерах любых типов.

5. Чем речь, передаваемая вокодерами, отличается от речи, передаваемой иными средствами?
6. Основной метод защиты информации в радиоканалах связи.
7. Чем звукоизоляция отличается от звукопоглощения?
8. Особенности распространения акустических волн в помещении.
9. Как влияет время реверберации на качество принимаемой речи?
10. Основные признаки закладных устройств, используемые для их обнаружения.
11. Методы поиска закладных радиоизлучающих устройств.
12. Методы поиска неизлучающих закладных устройств.
13. Методы поиска проводных телефонных закладных устройств.
14. Методы локализации закладных устройств.
15. Виды «чисток» помещения от закладных устройств.

# Глава 12. Экранирование побочных излучений и наводок

## 12.1. Экранирование электромагнитных полей

Для предотвращения утечки информации по радиоэлектронным техническим каналам утечки информации, вызванных ПЭМИН и радиозакладными устройствами, на опасных направлениях применяют электромагнитные экраны. Физические процессы при экранировании отличаются в зависимости от вида поля и частоты его изменения.

Различают электрические экраны для экранирования электрического поля, магнитные для экранирования магнитного поля и электромагнитные — для экранирования электромагнитного поля. Способность экрана ослаблять энергию полей оценивается **эффективностью экранирования** (коэффициентом ослабления). Если напряженность поля до экрана равна $E_0$ и $H_0$, а за экраном — $E_э$ и $H_э$, то $S_э = E_0 / E_э$ и $S_н = H_0 / H_э$. На практике эффективность экранирования измеряется в децибелах (дБ) и неперах (Нп): $S_{э(н)} = 20\lg[E_0(H_0) / E_э(H_э)]$ [дБ] или $S_{э(н)} = \ln[E_0(H_0) / E_э(H_э)]$ [Нп].

Аналитические зависимости эффективности экранирования определены для идеализированных (гипотетических) моделей экранов в виде бесконечно плоской однородной токопроводящей поверхности, однородной сферической токопроводящей поверхности и однородной бесконечно протяженной цилиндрической токопроводящей поверхности. Для других вариантов эффективность экранирования определяется с погрешностью, зависящей от степени их подобия гипотетическим.

1. При экранировании электрического поля электроны экрана под действием внешнего электрического поля перераспределяются таким образом, что на поверхности экрана, обращенной к источнику поля, сосредоточиваются заряды, противоположные по знаку зарядам источника, а на внешней (другой) поверхности экрана концентрируются одинаковые с зарядами источника поля (рис. 12.1).

Положительные заряды на рис. 12.1 создают вторичное электрическое поле, близкое по напряженности к первичному. С целью исключения вторичного поля, создаваемого зарядами на внешней поверхности экрана, экран заземляется и его заряды компен-

сируются зарядами земли. Экран приобретает потенциал, близкий потенциалу земли, а электрическое поле за экраном существенно уменьшается. Полностью устранить поле за экраном не удается из-за неполной компенсации зарядов на его внешней стороне вследствие ненулевых значений сопротивления в экране и цепях заземления, а также из-за распространения силовых линий вне границ экрана.

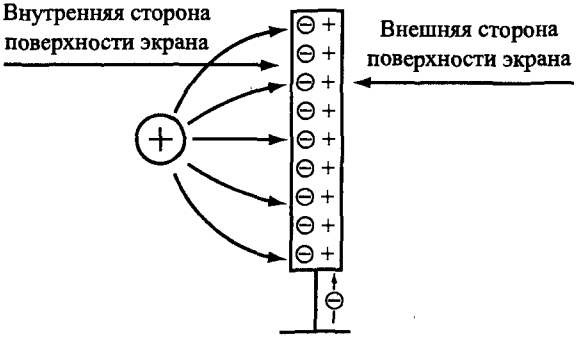



*Рис. 12.1.* Экранирование электрического поля

Эффективность экранирования зависит от электропроводности экрана и сопротивления заземления. Чем выше проводимость экрана и цепей заземления, тем выше эффективность электрического экранирования. Толщина экрана и его магнитные свойства на эффективность экранирования практически не влияют.

2. Экранирование магнитного поля достигается в результате действия двух физических явлений:

- «втягивания» (шунтирования) магнитных силовых линий поля в экран из ферромагнитных материалов (с $\mu >> 1$), обусловленного существенно меньшим магнитным сопротивлением материала экрана, чем окружающего воздуха;
- возникновением под действием переменного экранируемого поля в токопроводящей среде экрана индукционных вихревых токов, создающих вторичное магнитное поле, силовые линии которого противоположны магнитным силовым первичного поля.

Магнитное сопротивление пропорционально длине магнитных силовых линий и обратно пропорционально площади поперечного сечения рассматриваемого участка и величине магнитной прони-

цаемости среды (материала), в которой распространяются магнитные силовые линии. При втягивании магнитных силовых линий в экран уменьшается их напряженность за экраном. В результате этого повышается коэффициент экранирования.

При воздействии на экран переменного магнитного поля в материале экрана возникают также ЭДС, создающие в материале экрана вихревые токи в виде множества замкнутых колец. Кольцевые вихревые токи создают вторичные магнитные поля, которые вытесняют основное и препятствует его проникновению вглубь металла экрана. Экранирующий эффект вихревых токов тем выше, чем выше частота поля и больше сила вихревых токов.

Коэффициент экранирования магнитной составляющей поля представляет собой сумму коэффициентов экранирования, обусловленного рассмотренными физическими явлениями. Но доля слагаемых зависит от частоты колебаний поля. При $f = 0$ экранирование обеспечивается только за счет шунтирования магнитного поля средой экрана. Но с повышением частоты поля все сильнее проявляется влияние на эффективность экранирования вторичного поля, обусловленного вихревыми токами в поверхности экрана. Чем выше частота, тем больше влияние на эффективность экранирования вихревых токов.

В силу разного влияния рассмотренных физических явлений магнитного экранирования отличаются требования к экранам на низких и высоких частотах. На низких частотах (приблизительно до единиц кГц), когда преобладает влияние первого явления, эффективность экранирования зависит в основном от магнитной проницаемости материала экрана и его толщины. Чем больше значения этих характеристик, тем выше эффективность магнитного экранирования. Для экрана, например, в виде куба эффективность магнитного экрана можно оценить по формуле:

$$S_н \approx 1 - \mu d/D,$$

где $d$ — толщина стенок экрана; $D$ — размер стороны экрана кубической формы.

Эффективность экранирования за счет вихревых токов зависит от их силы, на величину которой влияет электрическая про-

водимость экрана. В свою очередь это сопротивление прямо пропорционально электрическому сопротивлению материала экрана и обратно пропорционально его толщине. Однако по мере повышения частоты поля толщина материала экрана, в которой протекают вихревые токи уменьшаются из-за так называемого поверхностного или скин-эффекта. Сущность его обусловлена тем, что внешнее (первичное) магнитное поле ослабевает по мере углубления в материал экрана, так как ему противостоит возрастающее вторичное магнитное поле вихревых токов. Напряженность переменного магнитного поля уменьшается по мере проникновения его в металл экрана на глубину x от его поверхности по экспоненциальному закону:

$$H_x = H_0 \exp(-x / \sigma),$$

где σ — эквивалентная глубина проникновения, соответствующая ослаблению напряженности магнитного поля в 2,72 раза и вычисляемая по формуле:

$$\sigma = 503\sqrt{\frac{\rho}{f\mu}},$$

где ρ — удельное электрическое сопротивление материала экрана в Ом · мм²/м; f — частота магнитного поля в Гц; μ — относительная магнитная проницаемость материала экрана.

Уменьшение эквивалентной глубины проникновения при увеличении μ обусловлено тем, что ферромагнитные материалы «втягивают» силовые магнитные линии первичного поля, в результате чего повышаются концентрация магнитных силовых линий и, следовательно, напряженность магнитного поля внутри материала экрана. В результате этого повышаются уровни индуцируемых в нем зарядов, следствием чего является увеличение значений вихревых токов и напряженности вторичного магнитного поля. Таким образом, глубина проникновения тем меньше, чем выше частота поля, удельная магнитная проницаемость и электрическая проводимость металла экрана.

На высоких частотах эффективность магнитного экранирования в дБ экраном толщиной d в мм можно определить, подставив в

$S_н = 20 \lg (H_х / H_0)$ выражение для $H_х$. В результате такой подстано ки и преобразования легко получить, что

$$S_н \approx 0{,}0173 d \sqrt{\frac{\mu f}{\rho}} .$$

Однако это выражение может использоваться для приближен ной оценки эффективности экранирования при условии, что значе ние d соизмеримо с σ. Если d >> σ, то из-за поверхностного эффект увеличение d слабо влияет на эффективность экранирования, та как вторичное магнитное поле создают вихревые токи в поверх ностном слое экрана.

Следовательно, для обеспечения эффективного магнитног экранирования на высоких частотах следует для экранов исполь зовать материалы с наибольшим отношением μ / ρ, учитывая пр этом, что с повышением f сопротивление из-за поверхностного эф фекта возрастает в экспоненциальной зависимости. На высоки частотах глубина проникновения может быть столь малой, а со противление столь велико, что применение материалов с высокой магнитной проницательностью, например пермаллоя, становит ся нецелесообразным. Для f > 10 МГц значительный экранирую щий эффект обеспечивает медный экран толщиной всего 0,1 мм Для экранирования магнитных полей высокочастотных контуро усилителей промежуточной частоты бытовых радио- и телевизи онных приемников широко применяют алюминиевые экраны, ко торые незначительно уступают меди по удельному электрическому сопротивлению, но существенно их легче. Для высоких частот тол щина экрана определяется в основном требованиями к прочност конструкции.

Кроме того, на эффективность магнитных экранов влияет кон струкция самого экрана. Она не должна содержать участков с от верстиями, прорезями, швов на пути магнитных силовых линий и вихревых токов, создающих им дополнительное сопротивление.

Так как магнитное экранирование обеспечивается за счет то ков, а не зарядов, магнитные экраны не нуждаются в заземлении.

3. Физические процессы при электромагнитном экранирова нии рассматриваются на модели, представленной на рис. 12.2.

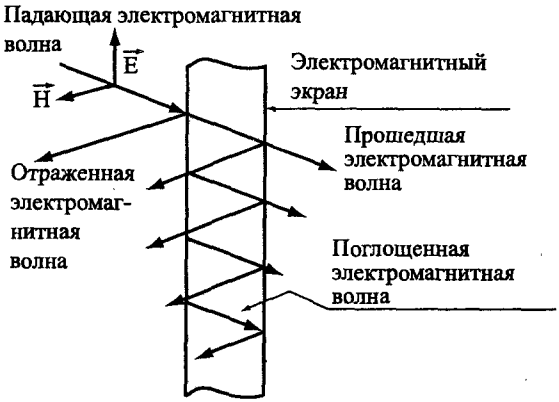



*Рис. 12.2.* Электромагнитное экранирование

Электромагнитное экранирование обеспечивается за счет отражения части от экрана и поглощения части, проникшей в экран электромагнитного поля. Следовательно, эффективность экранирования $S_э = S_{э,\,отр} + S_{э,\,погл}$, где $S_{э,\,отр} = \sum_{\forall i} S_{э,\,отр,\,i}$ — эффективность экранирования за счет отражения электромагнитной волны от поверхности экрана; $S_{э,\,погл} = \sum_{\forall i} S_{э,\,погл,\,i}$ —эффективность экранирования за счет поглощения электромагнитной волны в экране.

Эффективность экранирования в дБ за счет отражения электромагнитного поля рассчитывается по формуле:

$$S_{э,\,отр} \approx 151 - 10 \lg f\mu\rho.$$

Величина эффективности экранирования в дБ за счет поглощения в экране толщиной d мм оценивается по формуле:

$$S_{э,\,погл} \approx 0{,}0173d\sqrt{\frac{f\mu}{\rho}}.$$

Последнее выражение совпадает с приблизительной формулой, определяющей эффективность магнитного экранирования за счет вторичного поля. Это подтверждает утверждение, что поглощение электромагнитного поля обусловлено, прежде всего, потерями энергии вихревых токов в материале экрана.

Как следует из приведенных формул, в зависимости от часто ты, показателей магнитных и электрических свойств материала эк рана влияние отражения и поглощения на разных частотах сущест венно отличается. На низких частотах наибольший вклад в эффек тивность экранирования вносит отражение от экрана электромаг нитной волны, на высоких — ее поглощение в экране. Доля эти составляющих в суммарной величине эффективности электромаг нитного экранирования одинаковая для немагнитных ($\mu \approx 1$) экра нов на частотах в сотни кГц (для меди — 500 кГц), для магнитны ($\mu >> 1$) — на частотах в доли и единицы кГц, например для пер маллоя — 200 Гц. Магнитные материалы обеспечивают лучше экранирование электромагнитной волны за счет поглощения, а не магнитные, но с малым значением удельного сопротивления — за счет отражения.

Кроме того, учитывая, что электромагнитная волна содер жит электрическую и магнитную составляющие, то при электро магнитном экранировании проявляются явления, характерные дл электрического и магнитного экранирования.

Следовательно, на низких частотах материал для экрана дол жен быть толстым, иметь высокие значения магнитной проница емости и электропроводности. На высоких частотах экран должен иметь малые значения электрического сопротивления, а требова ния к его толщине и магнитной проницаемости материала сущест венно снижаются. Для обеспечения экранирования электрической составляющей электромагнитный экран надо заземлять.

## 12.2. Экранирование электрических проводов

Экранированием проводов решаются 2 задачи:

- уменьшение наводок на выходящие за пределы контролируе мой зоны провода от электромагнитных излучений основных и вспомогательных технических средств и систем;
- снижение уровня электромагнитных излучений проводов ин формационных линий основных и вспомогательных техничес ких средств и систем.

Физические основы экранирования с целью снижения пара зитных наводок на провода рассмотрены в предыдущем парагра

фе. В данном подразделе рассматриваются физические основы экранирования проводов кабелей.

Экранирование провода несимметричного кабеля производится путем размещения его в экране — металлической (железной, медной, цинковой, свинцовой) трубе и металлической сетчатой оплетке (плетенке). Для экранирования электрической составляющей экран заземляется (рис. 12.3).

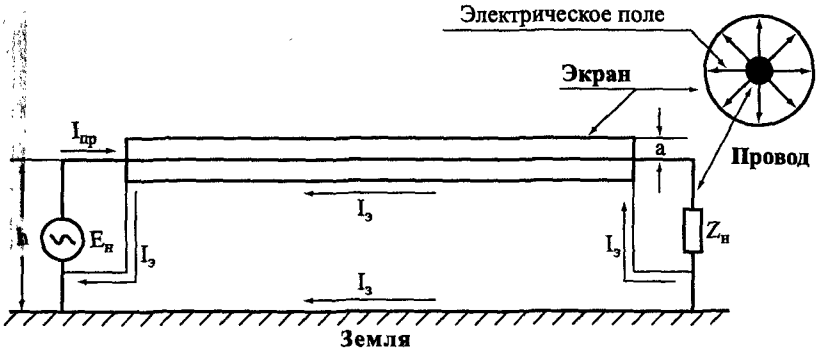



*Рис. 12.3.* Электрическое экранирование несимметричного кабеля

Заряды в проводе создают электрическое поле, силовые линии которого притягивают заряды к внутренней поверхности экрана. Возникающие в результате этого на внешней поверхности экрана заряды нейтрализуются зарядами земли. Электрическое поле вне экрана определяется малой величиной вторичного электрического поля, вызванного не полностью компенсированными зарядами на внешней поверхности экрана из-за конечного, не равного 0, сопротивления цепей заземления и экрана (от точки заземления до точки измерения). Чем больше точек заземления (многоточечное заземление), чем меньше электрическое сопротивление экрана и заземлителя, тем меньше величина напряженность вторичного электрического тока. Но, как правило, заземляются только концы экрана кабеля при подсоединении его к разъемам радиоэлектронных средств. Поэтому напряженность вторичного электрического поля повышается к середине такого кабеля и уменьшается к концам.

Источниками побочных излучений магнитного поля являются две магнитные рамки. Первая образуется цепью — провод и эк-

ран, по которому в соответствии с рис. 12.3 протекает ток $I_э$. Цепь второй рамки образуют тот же провод и токопроводящая поверхность земли, по которой в обратном направлении протекает ток $I_з$. Очевидно, что $I_{обр} = I_э + I_з = I_{пр}$. Мощность излучения рамок зависит от их площади и протекающих токов. Влияние экрана на уменьшение обратного тока в земле учитывается с помощью коэффициента токового экранирования $K_т$, равного отношению величины обратного тока в земле $I_з$ к суммарной величине обратного тока $I_{обр}$. Для способа экранирования на рис. 12.3 в диапазоне звуковых частот $K_т \approx 0{,}05$. В большинстве случаях расстояние от провода до экрана a значительно меньше расстояния провода до земли h. Поэтому площадь второй рамки значительно больше площади первой. Хотя ток $I_э > I_з$ из-за более высокой проводимости экрана, чем земли, но при h >> a побочное излучение рамки «провод-земля» является недопустимо большим. Для его снижения необходимо уменьшать h и ток $I_з$. Ток $I_з$ обеспечивается при отсутствии заземления экрана у нагрузки (рис. 12.4).

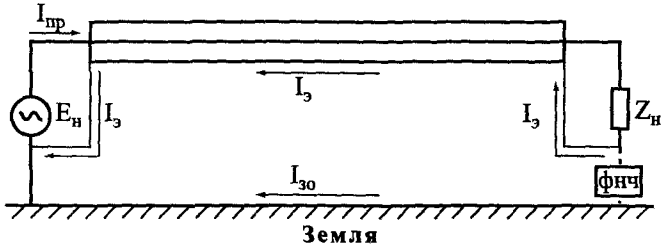



*Рис. 12.4.* Экранирование несимметричного кабеля

Но при этом из-за увеличения сопротивления заземления возрастает вторичное электрическое поле, создаваемое экраном. Поэтому на практике вариант заземления выбирают исходя из минимизации суммарного побочного излучения электрической и магнитной составляющих электромагнитного поля. Например, если ток $I_{пр}$ содержит постоянную составляющую, то целесообразно заземление экрана у нагрузки производить через фильтр низкой частоты, например через индуктивность, имеющую малое сопротивление для постоянного тока и большое — для переменного тока (рис. 12.4). В этом случае обеспечивается эффективное электрическое экранирование на низких частотах и магнитное экранирование

на высоких частотах, на которых вторая рамка может создавать существенное излучение.

Экранирование проводов симметричных кабелей с целью снижения излучений, вызванных несимметричностью проводов относительно иной токопроводящей поверхности или земли, производится аналогично рассмотренным способам.

Наибольший экранирующий эффект достигается при применении металлических водогазовых труб, достаточно большая толщина стенок которых обеспечивает большое ослабление магнитного поля на низких частотах. Более удобно прокладывать кабели в свинцовой оболочке, так как они обеспечивают возможность изгиба кабеля в любом месте трассы. Эти кабели обеспечивают высокую устойчивость против агрессивной среды и эффективное электрическое экранирование, Так как свинец относится к диамагнетикам (с $\mu < 1$), то магнитное экранирование достигается на высоких частотах, на которых наибольший экранирующий эффект достигается за счет вихревых токов. Еще большей эластичностью обладают экраны в виде оплетки из сетки, допускающей многократные перегибы. Оплетка перекрывает 60–90% поверхности изолированного провода. Но наличие отверстий в оплетке ухудшает магнитное экранирование по сравнению со сплошным экраном на 5–30 дБ.

Если экранирование проводов несимметричных кабелей представляет собой наиболее эффективный способ существенного снижения их побочных электромагнитных излучений, то для симметричных кабелей существуют иные и более дешевые способы. Они предусматривают меры, обеспечивающие более полную компенсацию полей, создаваемых токами противоположного направления в проводах (жилах) симметричного кабеля.

## 12.3. Компенсация полей

Низкочастотные и высокочастотные поля, создаваемые токами в симметричных кабелях, имеют почти равные напряженности и почти противоположные фазы. Побочные излучения проводов симметричных кабелей обусловлены разной удаленностью проводов от точки в пространстве, в которой производится измерение уровня излучения, и разными значения емкостей между провода-

ми и рассматриваемыми токопроводящими поверхностями, в том числе и землей. Эта разница вызывается разным расположением проводов в пространстве, конструктивными отличиями и неоднородностью материала проводов и их изоляции.

Компенсация полей проводов симметричного кабеля при его прокладке параллельно другим кабелям улучшается путем симметрирования проводов с помощью дополнительных емкостей или размещением жил в многожильном кабеле или жгуте таким образом, чтобы уменьшить их влияние друг на друга. Для этого измеряют емкости между проводами и установкой дополнительных конденсаторов $C_c$ добиваются равенства емкостей между рассматриваемыми проводами (рис. 12.5а)).

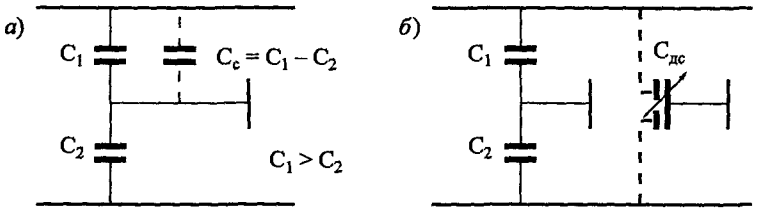



*Рис. 12.5.* Симметрирование проводов кабелей

Более удобные для симметрирования кабелей так называемые дифференциальные конденсаторы переменной емкости $C_{дс}$. (рис. 12.5). Путем вращения регулировочного винта такого конденсатора добиваются минимального уровня индикатора напряженности поля измерительного прибора, установленного в контролируемом месте. Подключение симметрирующих конденсаторов производится в специальных симметрирующих муфтах, которые включаются в разрыв кабеля (для длинных кабелей) или в соединительные разъемы.

При промышленном изготовлении многожильных кабелей предусматривается расположение жил одной группы на одинаковом расстоянии от жил другой группы. Это обстоятельство важно учитывать при монтаже кабеля. Для каждой цепи выбираются жилы, расположенные на равном расстоянии от жил других цепей.

Для компенсации полей, вызванных разной удаленностью проводов от точки пространства, производят скручивание проводов

бели. Кабель, состоящий из двух скрученных проводов, называ-
ют **витой парой** или **бифиляром**. Повышение компенсации по-
лезных проводов пары достигается тем, что поле в рассмат-
риваемой точке пространства представляет собой суперпозию по-
лей двух параллельных проводов с разным расстоянием от точ-
ки измерения, а полей от участков проводов длиной, соответству-
ющей шагу скрутки. Так как после каждой скрутки расположение
проводов проводов по отношению к точке измерения меняется на
противоположное (более близкий участок провода становится бо-
лее удаленным), то происходит существенно более полная компен-
сация полей от проводов с противоположным направлением тока.
Такой компенсации полей добиться не удается, но при достаточ-
но малом шаге скрутки ослабление излучения достигает приемле-
мых для практики значений, заметно не уступающих более доро-
гому экранированию. Например, при уменьшении шага скрутки
в 3 раза (с 55 до 18 мм) излучающая способность снижается при-
мерно на 30 дБ. Абсолютное значение ослабления излучения витой
пары с шагом около 2 мм достигает 80 дБ. Малая излучающая спо-
собность, меньшая стоимость и большая гибкость витой пары спо-
собствуют ее широкому использованию в качестве кабеля локаль-
ных сетей ЭВМ, размещаемых внутри одного здания.

В настоящее время используются неэкранированные кабели с витыми парами из медной проволоки (UTP — Unshilded Twisted Pair) и экранированные кабели с витыми парами из медной проволоки (STR — Schilded Twisted Pair). Чаще используются кабели STR 3-й, 4-й, и 5-й категорий. Кабели 3-й категории обеспечивают скорость передачи до 10 Мбит/с, 4-й категории — до 25 Мбит/с, 5-й категории — до 155 Мбит/с.

Для увеличения ослабления излучения витую пару помещают в экран. Экранированная витая пара эффективна на частотах до 100 кГц, но на частотах более 1 МГц в ней существенно возрастают потери. В качестве экранированной витой пары используют также скрутку из трех проводов (**трифиляр**), по двум из которых передаются сигналы, а третий заземляется. Эффективность экранированного кабеля может быть более 100 дБ.

## 12.4. Предотвращение утечки информации по цепям электропитания и заземления

Меры по предотвращению утечки защищаемой информации по цепям электропитания должны:

- устранить проникновение сигналов с защищаемой информации через блоки электропитания основных технических средств и систем в цепи электропитания;
- снизить до допустимого уровня наводки НЧ и ВЧ излучений с защищаемой информацией на провода цепей электропитания;
- подавить электрические сигналы в цепях электропитания до выхода их из контролируемой зоны.

Гальваническая связь блока питания с информационными блоками РЭС обеспечивается через фильтр низкой частоты, который уменьшает до приемлемых значений уровень переменной составляющей напряжения с выхода блока питания РЭС. Чем меньше величина переменной составляющей (пульсаций), тем выше качество блока питания. Однако снижение коэффициента пульсации связано с резким ростом затрат и увеличением масса-габаритных характеристик блока питания. Для допустимых значений пульсации напряжения типовых блоков питания полоса его пропускания $\Delta F$ составляет около 30 Гц. При таком значении возможно пропускание огибающей речевого сигнала в цепи электропитания. Уменьшение $\Delta F$ достигается с помощью:

- дополнительных стабилизаторов в блоке питания;
- мотор-генератора;
- автономных источников питания (аккумуляторов, дизель-генераторов).

Мотор-генератор представляет собой генератор электрического тока, вращение ротора которого обеспечивается электрическим двигателем, питаемым от первичного источника переменного тока. Полоса пропускания мотор-генераторов составляет доли Гц, что исключает проникновение информации от потребителя электропитания к первичному источнику. Мощность мотор-генераторов составляет 8–75 кВА.

Для устранения проникновения опасных сигналов в цепи электропитания через емкостные и индуктивные связи блока питания применяют способы, направленные на снижение значений этих па-

разитных связей. С этой целью изменяют компоновку (взаимное расположение) деталей блока питания таким образом, чтобы минимизировать длину токопроводящих параллельных элементов и увеличить между ними расстояние, а также экранируют излучающие поля детали. Наибольшие паразитные связи возникают между первичной и вторичной обмотками силового трансформатора, преобразующего напряжения первичного источника питания в напряжения питания элементов схемы радиоэлектронного средства. С целью снижения их до допустимых значений применяют следующие способы:

- первичную и вторичную обмотку располагают на разных частях магнитопровода сердечника трансформатора;
- между первичной и вторичной обмотками, размещаемыми на одной катушке, устанавливается заземленный экран из медной фольги толщиной не менее 0,2 мм;
- первичная обмотка размещается в заземленном экране;
- обмотки трансформатора размещаются в индивидуальные заземленные экраны, между которыми также устанавливается заземленный экран.

В первом варианте снижается кпд трансформатора из-за дополнительного рассеяния магнитного поля первичной обмотки в воздухе. Экран преобразует паразитную емкость между проводами обмоток в паразитные емкости между этими проводами и заземленным экраном. Чтобы исключить образование вокруг магнитопровода короткозамкнутого витка из экрана, в котором в результате магнитной индукции поля первичной обмотки возникнут большие вихревые токи, между концами экрана оставляют воздушный зазор с очень высоким сопротивлением.

В целях активного подавления опасных сигналов, проникающих через блоки питания и наводимые в проводах силовых кабелей, цепи электропитания зашумляют. Для этого подается в провода силовых кабелей речеподобный шумовой сигнал, который формируется из белового шума с помощью соответствующих фильтров.

Для исключения распространения высокочастотных опасных сигналов по цепям электропитания при их выводе из выделенных помещений устанавливаются фильтры питания, линейные и развязывающие сетевые фильтры. Фильтры питания обеспечивают за-

тухание опасных сигналов в полосе 20 кГц–1 ГГц не менее 60 дБ. Они выпускаются на рабочее напряжение 127–500 В и рабочий ток 1–70 А. Так как в фильтрах, пропускающих большой ток, применяются индуктивности (катушки) из толстого провода, то вес их может достигать десятки кг.

Кроме указанных технических мер для предотвращения утечки информации по цепям электропитания необходимо обеспечить следующие требования и рекомендации к системе электропитания организации:

- электрические установки и кабели должны быть установлены в пределах контролируемой зоны;
- на объектах 1-й категории электропитание осуществляется от устройств, обеспечивающих электромагнитную развязку сети электропитания от промышленной электросети, в том числе сертифицированные агрегаты бесперебойного питания, 4-проводные сетевые помехоподавляющие фильтры, системы двигатель-генератор;
- на объектах 2-й категории электропитание производится через сертифицированные сетевые помехоподавляющие фильтры и (или) проводится активное зашумление цепей электропитания;
- на объектах 3-й категории электропитание может осуществляться от подстанции в контролируемой зоне без дополнительных мер;
- на объектах 2-й и 3-й категорий допускается электропитание от трансформаторной подстанции, размещенной за пределами контролируемой зоны, но при использовании сертифицированных 4-проводных помехоподавляющих фильтров или систем активного зашумления;
- подача электроэнергии от трансформаторной подстанции до силовых щитов производится экранированным силовым кабелем, а распределительные устройства и силовые щиты закрываются на замок и опечатываются.

Меры по предотвращению утечки информации по цепям заземления направлены на снижение величины паразитной гальванической связи между заземляемыми радиоэлектронными средствами и уменьшением площади магнитных рамок, образуемых цепями заземления. При этом эти используемые меры не должны увеличивать сопротивление цепей заземления.

При выборе схемы заземления следует учитывать, что наиболее часто используемое последовательное заземление (рис. 12.6 а)) имеет наибольший коэффициент гальванической паразитной связи. Низкочастотные средства, размещенные на небольшом расстоянии друг от друга, рекомендуется заземлять в одной точке (рис. 12.6 б)), в остальных случаях целесообразно применять многоточечное заземление (рис. 12.6 в)).

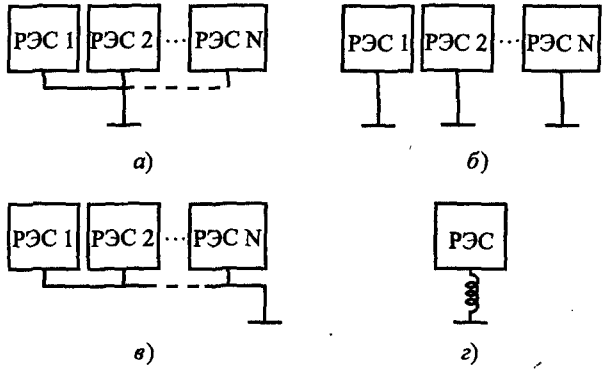



*Рис. 12.6.* Типы заземлеиия радиоэлектронных средств

С целью исключения снятия информации с токов, растекающихся в земле, заземлители размещаются внутри контролируемой зоны на удалении не менее 2–3 м от ее границы (забора).

## Вопросы для самопроверки

1. Условия эффективного экранирования электрического поля.
2. Условия эффективного экранирования магнитного поля на низких частотах.
3. Условия эффективного экранирования магнитного поля на высоких частотах.
4. Условия эффективного экранирования электромагнитного поля.
5. Особенность экранирования несимметричного кабеля.
6. Каким образом производится симметрирование кабелей?
7. Меры по предотвращению утечки защищаемой информации по цепям электропитания.
8. Требования к средствам электропитания объектов 1–3 категорий.
9. Каким образом предотвращают утечку информации по цепям заземления радиоэлектронных средств?

# Глава 13. Методы предотвращения утечки информации по вещественному каналу

Методы предотвращения утечки информации по вещественному каналу можно разделить на две группы:

- методы защиты информации в отходах деятельности организации;
- методы защиты демаскирующих веществ в отходах химического производства.

## 13.1. Методы защиты информации в отходах производства

Защита информации на бумажных (машинных) носителях и содержащейся в отходах и браке научной и производственной деятельности организации предусматривает следующие меры:

- учет отдельных листков с записями, использованной копировальной бумаги, макетов, бракованных узлов и деталей;
- сбор черновиков документов и различных записей на отдельных неучтенных листках в специальные опечатанные ящики;
- уничтожение бумажных и стирание (уничтожение) машинных носителей;
- разборка макетов и блоков, разрушение механических деталей.

Учет и сбор отдельных несекретных листов с записями, рисунками, схемами и другой информацией, не подлежащей свободному распространению, предусматривает указание на нем порядкового номера и номера папки, в которой он должен храниться. Каждая такая папка содержит опись хранящихся в ней документов. При изъятии документа при его передаче или уничтожении в описи папки делается соответствующая запись с указанием числа и подписи ответственного лица. При отсутствии в помещении уничтожителей бумаг бумажные носители, не подлежащие длительному хранению, собираются в опечатанные печатью ответственного исполнителя, например старшего по помещению, деревянные или металлические ящики с прорезью. После заполнения ящиков бумага из них изымается и уничтожается.

В настоящее время вместо сжигания подлежащих уничтожению бумажных носителей все шире применяют различные измельчители бумаги (to scred — **шредеры**). Они удобны в работе, занимают сравнительно мало места, экологически безвредны.

По производительности (количеству одновременно измельчаемых листов бумаги) различают **индивидуальные** (до 12 листов), **офисные** (до 50 листов) и **центральные** (до 500 листов) **шредеры**. В зависимости от размеров фрагментов измельченной бумаги шредеры различаются степенями секретности:

- первая степень — продольная резка шириной до 12 мм и неограниченной длины;
- вторая степень — параллельная и перекрестная резка полосками шириной до 6 мм и неограниченной длины;
- третья степень — перекрестная резка на фрагменты шириной менее 4 мм и длиной до 80 мм или параллельная резка на полоски шириной до 2 мм;
- четвертая степень — перекрестная резка на фрагменты шириной менее 2 мм и длиной менее 15 мм;
- пятая степень — перекрестная резка на фрагменты шириной менее 0,8 мм и длиной менее 13 мм.

Для уничтожении конфиденциальных документов используют шредеры 3-й степени секретности, для документов, содержащих государственную тайну, — шредеры 4-й и 5-й степени.

Гарантированное уничтожение информации обеспечивают дробители (**гриндеры**), измельчающие бумагу в мелкие клочки. В них можно менять размеры клочков и регулировать скорость. Гребенчатый гриндер, имеющий два вращающихся гребня, ворошит бумагу, обеспечивая непрерывность процесса, в то время как искромсанная до необходимых размеров бумага проваливается через сетку в нижнюю часть машины.

Наибольшее измельчение бумаги достигается в так называемых **дезинтеграторах**, которые способны порезать бумагу на кусочки до 1 мм, т. е. до размеров, когда невозможно разобрать отдельную букву. Деинтеграторы применяют в банках также для уничтожения денег.

Так как все шире в качестве вторичных носителей информации используются машинные носители информации (гибкие и жесткие

магнитные диски, оптические диски, флэш-память и др.), то существует проблема уничтожения информации на них без даже теоретической возможности ее восстановления.

Вышедшие из строя винчестеры, не читаемые гибкие и оптические диски, на которых хранилась защищаемая информации, после механического разрушения, а иногда и без него, выбрасываются на свалку. Кроме того, работоспособные винчестеры и гибкие магнитные диски могут многократно перемещаться от одного компьютера к другому. Например, после модернизации компьютера, относящегося к основному средству, винчестер заменяется на новый большего объема, а предварительно стертый старый винчестер устанавливается на другой компьютер, на котором не предусматривается обработка секретной информации. После стирания информации штатными средствами вычислительной техники на магнитных носителях информации остаются следы предыдущих записей, по которым возможно восстановление фрагментов информации. Для гарантированного стирания информации созданы и применяются средства, создающие существенно большие поля стирания, чем способны создать головки дисководов. Такие средства называются **разрушителями**.

Если информацию на магнитных носителях можно стереть глубоким форматированием, то на нечитаемых оптических дисках должен полностью физически уничтожаться информационный слой. Гарантированное уничтожение информации на этих дисках путем их механического разрушения не достигается, так же как невозможно полностью уничтожить информацию на листе бумаги, разорвав его вручную на куски. CD-ROM диски утилизируют нагреванием до расплавления или захоронением в воде или земле. Для оперативного уничтожения информации на оптических дисках разработан пиротехнический способ. Для его реализации на поверхность диска наносится тонкий слой пиротехнического состава, поджигаемого электрическим импульсом во время нахождения диска в дисководе. После поджигания поверхность диска разогревается в течение нескольких секунд до температуры около 2000° С, но повреждение дисковода при этом не происходит.

Для защиты информации, содержащейся в макетах, в узлах и элементах бракованной продукции, необходимо производить их учет, а после использования — разбирать и уничтожать неразборные узлы и части, обладающие демаскирующими признаками.

## 13.2. Методы защиты демаскирующих веществ в отходах химического производства

Классификация методов защиты демаскирующих веществ приведена на рис. 13.1.


*Рис. 13.1.* Классификация способов защиты демаскирующих веществ

Способы защиты демаскирующих веществ предусматривают применение мер, обеспечивающих уменьшение их концентрации до значений, исключающих определение злоумышленниками структуры и свойств демаскирующих веществ путем физического и химического анализа. Основные направления снижения концентрации демаскирующих веществ — внедрение безотходных или малоотходных технологий, а также глубокая очистка отходов и выбросов.

Наиболее экономичным направлением защиты демаскирующих веществ в отходах — использование отходов в качестве вторичного сырья для создания иной продукции на этом же предприятии. Острота проблемы защиты возрастает, если промежуточные продукты с демаскирующими веществами не находят применение на одном предприятии. Для продажи их в качестве вторичного сы-

рья, а также выброса на свалку, в водоемы или атмосферу отходы
интересах защиты информации надо очистить от демаскирующи
веществ, т. е. уменьшить концентрацию демаскирующих веществ
до допустимых значений.

Выбор метода и способа очистки отходов от демаскирующи
веществ зависит, прежде всего, от видов (твердое, жидкое, газообразное) демаскирующих веществ и других веществ (примесей) в отходах. В качестве основных методов очистки отходов от демаскирующих веществ применяются методы механической очистки (фильтрация), нагрев, охлаждение и химическая обработка.

**Фильтрация демаскирующих веществ** осуществляется в аппаратах объемного улавливания (в циклонах, электрических фильтрах и др.), в результате абсорбции и адсорбции (поглощения всем объемом и поверхностью вещества соответственно), центрифугирования, промывки, разделения по удельной плотности, магнитным свойствам и т. д.

**При нагревании** очистка отходов от демаскирующих веществ происходит путем пиролиза (расщепления органических веществ на более простые), крекинга (разложения нефтепродуктов), испарения, дегазификации, выпарки, сушки, прокалки, отгонки, сжигания и др. процессов, в результате которых удается отделить демаскирующее вещество от иных примесей или превратить его в вещество, информация о котором не подлежит защите.

**При охлаждении** отходов для выделения демаскирующих веществ используются процессы конденсации газообразных веществ, вымораживания жидкостей и др.

Превращение отходов с демаскирующими веществами в нейтральные, информация о которых не требует защиты, возможно также путем их **химической обработки**, в ходе которой на отходы воздействуют химическими веществами, вступающими с ними в **химические реакции**.

Отходы, очистка от демаскирующих признаков которых указанными методами невозможна или экономически нецелесообразна, подлежат **захоронению**.

Выделенные демаскирующие вещества собираются в соответствующие емкости и подвергаются последующей обработке для нейтрализации или захоронения. Неиспользуемые радиоактивные

ществ не могут быть нейтрализованы и подлежат захоронению на специальных могильниках.

### Вопросы для самопроверки

1. Как уничтожаются бумажные носители информации?
2. Почему надо защищать информацию об отходах производства?
3. Преимущества замкнутых циклов производства с точки зрения обеспечения защиты информации.
4. Методы очистки отходов производства в интересах защиты информации.
5. Способы фильтрации демаскирующих веществ.
6. Когда осуществляют захоронение отходов?

### Основные положения раздела II

1. Любой объект может быть описан набором видовых, сигнальных и вещественных признаков. Когда объект взаимодействует с другими объектами, то при их взаимодействии признаки изменяются. Это изменение можно интерпретировать как результат передачи информации от одного объекта к другому. Следовательно, полученная объектом информация соответствует разности его признаков после и до взаимодействия его с другими объектами. Информация переносится веществом или энергией в виде значений их параметров — признаков. Такая информация представляется на языке признаков и является первичной. Материальные объекты, поля и микрочастицы, информационные параметры которых содержат информацию, являются ее носителями. Вторая сигнальная система человека способна отображать (кодировать) набор признаков в виде абстрактных символов национальных и профессиональных языков. Такая информация является вторичной и называется семантической.

Информация как предмет защиты имеет следующие свойства, которые следует учитывать при ее защите:

- так как информация не материальна, то объектом защиты являются ее носители, а сама информация — предметом защиты;
- ценность информации определяется ее полезностью для ее владельца (пользователя);

- информация является товаром, ее цена характеризуется полез ностью информации для участников рынка и складывается и себестоимости и прибыли;
- цена и ценность информации изменяются во времени, как пра вило, уменьшаются. Но возможен их рост во времени, например исторических документов;
- невозможно объективно, без учета полезности для пользовател (владельца) определить количество информации, поэтому для оценки количества информации используются косвенные, так называемые объемные меры;
- информация способна к «растеканию» в пространстве, между людьми, для ее локализации необходим дополнительный ресурс;
- при копировании информации ее количество (объем) не меняется, а цена уменьшается.

2. Любая информация может быть отнесена к семантической или информации о признаках материального объекта — к признаковой информации. Семантическая информация, циркулирующая в человеческом обществе, отображает создаваемые образы и модели с помощью символов на языках общения людей (национального общения и профессиональных). Признаковая информация описывает конкретный материальный объект на языке его признаков. Признаки, позволяющие отличить один объект от другого, называются демаскирующими. Демаскирующие признаки объекта, характеризующие его состояния, разделяют на опознавательные и признаки деятельности. Демаскирующие признаки о характеристиках объекта делятся на видовые (о внешнем виде), сигнальные (о характеристиках сигнала) и вещественные (о характеристиках веществ). По информативности демаскирующие признаки можно классифицировать на именные, прямые и косвенные. Именные и прямые демаскирующие признаки принадлежат рассматриваемому объекту, косвенные — другому объекту, на котором остаются следы взаимодействия с рассматриваемым объектом. Информативность оценивается величиной в интервале 0–1, которая характеризует индивидуальность признака. Информативность признака объектов генеральной совокупности соответствует вероятности обнаружения объекта по этому признаку.

Так как информация не материальная, то она может храниться, передаваться и обрабатываться, если она содержится на материальном носителе. Источниками семантической информации являются носители информации (субъекты и объекты), от которых можно получить информацию с возможностью определения оценки ее реквизитов, в том числе достоверности. К ним относятся люди, документы, продукция, измерительные датчики и приборы, отходы производства, материалы и технологическое оборудование. Источниками признаковой информации являются рассматриваемые объекты.

3. Угроза безопасности информации представляет собой состояние или действие взаимодействующих с носителями информации объектов и сил материального мира, которые могут привести к ее изменению, уничтожению, хищению или блокированию. Угрозы создаются внешними преднамеренными и случайными воздействиями злоумышленников и случайно возникающих сил, а также несанкционированным распространением носителя информации в пространстве. Внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести ее к хищению, образуют канал несанкционированного доступа. Несанкционированное распространение носителей с информацией от ее источника к злоумышленнику называется утечкой информации. Источниками преднамеренных угроз могут быть органы зарубежной разведки, разведки коммерческих структур внутри государства, криминальные структуры, завербованные, психически больные или недовольные своим положением сотрудники организации. К источникам случайных угроз воздействия относятся стихийные силы, приведшие в негодное состояние элементы инфраструктуры мест работы средств информационного обеспечения, технические средства с неисправными элементами, программы с ошибками и вирусами, неквалифицированные или плохо выполняющие свои обязанности операторы и обслуживающий персонал, грызуны и насекомые в местах размещения радиоэлектронных средств. Источниками угроз утечки являются люди и источники сигналов.

4. Носители защищаемой информации в виде сигналов, которые могут быть перехвачены злоумышленником и с которых мо-

жет быть снята информация, называются опасными. Опасные сигналы создаются техническими средствами в результате побочных электромагнитных излучений и наводок (ПЭМИН) в этих средствах. Побочные электромагнитные излучения и наводки включают нефункциональные акустоэлектрические преобразоваиия, побочные низкочастотные и высокочастотные излучения электромагнитного поля, паразитные связи и наводки в цепях радиосредств и электрических приборов.

По способу действия акустоэлектрические преобразователи делятся на активные (электродинамические, электромагнитные и пьезоэлектрические) и пассивные (параметрические) — индуктивные, магнитострикционные и емкостные (конденсаторные).

Низкочастотные опасные сигналы создаются электрическими сигналами в звуковом диапазоне в цепях основных и вспомогательных технических средств и систем. Высокочастотные излучения генерируются гетеродинами радиоприемников и телевизоров, генераторами стирания и подмагничивания магнитофонов, цепями (усилителями, дискретными устройствами), в которых возникает паразитная генерация, люминофором электронно-лучевых трубок мониторов. Напряженность электрической и магнитной компонент электромагнитного поля в ближней зоне излучения, расстояние r границы которой от источника излучения существенно меньше длины волны ($r < \lambda/2\pi$), убывает в зависимости от вида излучателя пропорционально $1/r^3$ и $1/r^2$. Простейшими излучателями являются магнитная рамка и вибратор. Магнитная рамка излучает поле, в которой преобладает магнитная компонента, вибратор — с преобладанием электрической компоненты. В переходной зоне, размеры которой $\lambda/2\pi < r < 1{,}5\lambda/\pi$ напряженность электромагнитного поля убывает пропорционально $1/r^2$. В дальней зоне ($r > 1{,}5\lambda/\pi$) электромагнитное поле распространяется в виде плоской волны, напряженность которой уменьшается обратно пропорционально r.

Паразитные связи в радиотехнических цепях, возникающие из-за побочного влияния магнитного поля одних цепей на другие, называются индуктивными, в результате побочного влияния электрического поля — емкостные, из-за проникновения побочных электрических сигналов в другие цепи в результате гальванического контакта — гальванические.

Побочные электромагнитные излучения создают угрозы безопасности информации и вызывают ее утечку из технических средств и систем, в том числе по цепям электропитания и заземления.

5. Утечка информации по сравнению с утечкой материальных тел имеет ряд особенностей: при ее утечке не выполняются законы сохранения вещества и энергии, утечка происходит при попадании информации к злоумышленнику, при утечке информации цена ее уменьшается. Возможность утечки информации характеризуется риском утечки, деятельность по изменению возможности утечки называется управление риском. Физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику образует технический канал утечки информации. Если информацию переносит сигнал, то технический канал включает источник сигнала, среду распространения и приемник сигнала. Канал, носителем информации в котором является вещество, состоит из источника информации, среды распространения и несанкционированного получателя. Технические каналы утечки информации по виду ее носителя делятся на оптические, акустические, радиоэлектронные и вещественные, по структуре — на простые и составные, по времени функционирования — на постоянные, эпизодические и случайные. Основными показателями технических каналов являются: пропускная способность, длина и относительная информативность.

Источник сигнала технического канала утечки информации характеризуется мощностью сигнала, параметрами спектра сигнала (шириной, неравномерностью спектральных составляющих), диаграммой направленности излучения сигнала, динамическим диапазоном сигнала. Среда распространения технического канала утечки информации характеризуется набором физических параметров, определяющих условия распространения носителя с информацией: скоростью распространения, коэффициентом передачи энергии носителя, амплитудно-частотной характеристикой, видом и мощностью помех. Основными параметрами приемника сигналов являются: диапазон принимаемых частот, чувствительность, пространственная селективность приемной антенны, динамический диапазон сигнала, вид и уровень искажений сигнала.

Повышение достоверности добываемой информации достигается комплексным использованием различных каналов.

6. Источниками сигналов акустических каналов утечки информации могут быть говорящий человек, технические средства звуковоспроизведения и механические узлы технических средств и машин. Среда распространения акустического канала утечки информации — воздух, вода, твердые тела. В качестве акустоэлектрического преобразователя приемника акустических сигналов могут использоваться микрофон (для воздушной среды), стетоскоп и акселерометр (для твердой среды), гидрофон (для водной среды) и геофон (для земной поверхности). Частоты акустические сигналов расположены в инфразвуковом, звуковом и ультразвуковом диапазонах частот, речевого сигнала в стандартном телефонном канале — 300–3400 Гц. Относительный (к мощности $10^{-12}$ Вт) уровень громкости звука составляет 0–130 дБ, уровень громкости разговора в служебном помещении составляет 40–70 дБ. Скорость распространения акустической волны в зависимости от вида среды распространения колеблется от 320 до 5 тысяч и более м/с.

Затухание акустической волны в среде распространения зависит от многих факторов, основными из которых являются плотность и упругость вещества среды, ее неоднородность. Наибольший коэффициент затухания акустической волны имеет воздушная среда, в воде он приблизительно на три порядка меньше, в твердых телах — еще меньше. На границе сред с разной плотностью акустическая волна частично переходит из одной среды в другую, частично отражается. В помещении за счет многократных отражений акустической волны от стен возникает явление послезвучания, которое называется **реверберацией** и измеряется временем уменьшения энергии звуковой волны на 60 дБ после момента прекращения работы ее источника. Для любого помещения существует оптимальное время реверберации, при котором обеспечиваются наилучшее восприятие акустических сигналов.

Для увеличения дальности подслушивания применяют специальные акустические приемники, имеющие остронаправленные микрофоны, и ретрансляторы речевых сигналов. В качестве ретрансляторов используют различные закладные устройства, паразитные акустоэлектрические преобразователи в радиоэлектрон-

ных средствах и электрических приборах, лазерные средства и средства ВЧ-навязывания.

7. В оптических каналах утечки информации источниками сигналов являются отражающие или излучающие объекты наблюдения. Освещенность объектов наблюдения в видимом (0,4–0,76 мкм) и инфракрасном (0,76–14 мкм) диапазонах составляет $10^{-5}$–$10^{5}$ лк. Средой распространения света могут быть воздух, безвоздушное пространство (космос), вода и оптическое волокно. Сложный состав атмосферы вызывает неравномерность амплитудно-частотной характеристики этого вида среды распространения. Участки с малым коэффициентом затухания называются окнами прозрачности. Прозрачность атмосферы оценивается метеорологической дальностью видимости. Метеорологическая дальность при очень сильном тумане составляет менее 50 м, при исключительно хорошей видимости — более 50 км. Среда распространения оптических сигналов в виде волоконно-оптических линий связи все шире используется в каналах связи, так как светопроводы устойчивы к внешним помехам, имеют малое затухание, долговечны, обеспечивают значительно большую безопасность передаваемой по волокну информации. Для передачи оптических сигналов применяются одномодовые и многомодовые волокна. Оптическое волокно характеризуется коэффициентом затухания и дисперсией.

Для наблюдения используются разнообразные оптические приемники: визуально-оптические, фото- и киноаппараты, приборы ночного видения и тепловизоры, а также телевизионные средства наблюдения.

8. В радиоэлектронном канале утечки информации производится добывание семантической информации, видовых и сигнальных демаскирующих признаков. Источниками сигналов являются передающие устройства, источники ПЭМИН, объекты, отражающие внешние электромагнитные поля, и источники собственных тепловых излучений в радиодиапазоне. Радиоэлектронные каналы утечки информации разделяются на каналы первого и второго рода. В каналах утечки 1-го рода производится добывание информации, передаваемой по функциональному каналу связи, в каналах 2-го вида источники сигналов случайные или создаваемые злоумышленником. Мощность источников каналов 1-го вида колеб-

лется от долей Вт до миллионов Вт, каналов 2-го вида — от долей мВт до единиц Вт.

Средой распространения сигналов радиоэлектронных каналов являются атмосфера, безвоздушное пространство и направляющие — электрические провода и волноводы. Радиоволны в зависимости от характера распространения в атмосфере делятся на земные (поверхностные), прямые, тропосферные и ионосферные. С повышением частоты колебаний радиосигналов увеличивается пропускная способность каналов утечки информации, повышается затухание сигналов в атмосфере, уменьшается уровень помех в среде распространения. Длинные и средние волны распространяются вдоль земной поверхности и пространственными лучами, короткие за счет многократных преломлений в ионосфере и отражений от земной поверхности могут огибать земной шар, ультракороткие — в пределах прямой видимости. Электрические сигналы распространяются по направляющим линиям связи, которые делятся на металлические (воздушные, кабели, волноводы), металло-диэлектрические и диэлектрические. Для радиоэлектронных каналов характерны разнообразные естественные и искусственные помехи. Естественные помехи имеют земное и внеземное происхождение, искусственные помехи могут быть непреднамеренными и преднамеренными.

9. Источниками информации в вещественных каналах утечки информации являются черновики различных документов и макеты разрабатываемых средств, отходы дело и промышленного производства, испорченные машинные носители информации, бракованная продукция, радиоактивные вещества. Перенос информации в этом канале возможен людьми и управляемыми ими техническими средствами, воздушными массами атмосферы, жидкой средой, радиоактивными излучениями.

10. Профессионально добывание информации осуществляют органы разведки — государственной и коммерческой. Информацию с помощью технических средств добывает техническая разведка. Техническая разведка по виду носителя добываемой информации делится на акустическую, оптическую, радиоэлектронную, компьютерную, химическую, радиационную, магнитометрическую, сейсмическую. Акустическая, оптическая и радиоэлектрон-

ная разведки состоят из многочисленных подвидов. Акустическая разведка по виду среды распространения акустической волны делится на воздушно-акустическую (акустическую), гидроакустическую и виброакустическую. Оптическая разведка включает визуально-оптическую, фотографическую, оптико-электронную (телевизионную, инфракрасную, лазерную) подвиды разведки. Радиоэлектронная разведка по виду добываемой информации разделяется на радио-, радиотехническую, радиолокационную, радиотеплолокационную и разведку ПЭМИН. По виду носителя средств разведки техническая разведка делится на наземную, воздушную, космическую и морскую.

Силы и средства технической разведки образуют систему технической разведки, включающей органы планирования и управления, добывания и информационной работы. Технология добывания информации включает процессы организации разведки (постановку задачи органу разведки, планирование разведывательной операции, постановку задач исполнителям, нормативное и оперативное управление), добывание данных и сведений (поиск объекта разведки, установление разведывательного контакта органа разведки с ее объектом, получение данных и сведений, передачу их в органы информационной разведки) и информационную работу (сбор данных и сведений, видовую и комплексную обработку, оформление и передачу заказчикам отчетных документов). При видовой обработке поступающие данные на языке признаков преобразуются в сведения на профессиональном языке, которые дополняются и обобщаются при комплексной обработке. При синтезе информации используются логические, структурные и статистические методы обработки данных и сведений.

11. Возможности добывания информации технической разведкой зависят от способов доступа к ней злоумышленника и его технических средств, обеспечивающих условия разведывательного контакта. Условия разведывательного контакта предусматривают знание злоумышленником местонахождения источника информации (пространственное условие), совпадение времени добывания с временем возможности доступа к информации (временное условие) и превышение в точке приема энергии носителя информации над помехами, достаточное для добывания органом разведки

(злоумышленником) информации с допустимым качеством (энергетическое условие). Способы доступа органа разведки (злоумышленника) к ее объекту предусматривают физическое проникновение злоумышленника к источнику информации, сотрудничество злоумышленника с представителем оргаиизации, имеющим доступ к информации, и дистанционный съем информации с носителя. Физическое проникновение к источнику информации возможно путем скрытого или с применением силы проникновения злоумышленника к месту хранения источника, а также в результате внедрения злоумышленника в организацию. Сотрудник организации привлекается к сотрудничеству путем его инициативного сотрудничества, его подкупа, сотрудничества под угрозой. Дистанционное добывание информации предусматривает съем ее с носителей, распространяющихся за пределы помещения, здания, территории организации, государства. Оно обеспечивается в результате наблюдения, подслушивания, перехвата, сбора носителей информации в виде материальных тел за пределами организации.

Информация без нарушения государственной границы добывается путем наблюдения объектов и перехвата радиосигналов техническими средствами, установленными на космических аппаратах, самолетах-разведчиках и разведывательных морских кораблях, а также перехвата радиосигналов наземными станциями радио- и радиотехнической разведки. Наибольшие возможности по добыванию информации обеспечивает космическая разведка (на низкоорбитальных космических аппаратах) и радио- и радиотехническая разведка, станции которых установлены на горах возле государственной границы.

Добывание информации без нарушения контролируемой зоны организации возможно путем наблюдения, подслушивания, перехвата сигналов и сборов отходов дело- и промышленного производства за пределами организации с помощью технических средств наземной разведки.

12. Методы инженерно-технической защиты информации объединяют методы физической защиты источников информации, скрытия информации и ее носителей, а также методы нейтрализации нефункциональных источников опасных сигналов. Физическая защита обеспечивается инженерной защитой (с по-

щью инженерных конструкций), техническими средствами охраны, обнаруживающими внешние воздействия, и их нейтрализацией. Методы скрытия информации направлены на снижение допустимых значений вероятностей обнаружения и распознавания носителей информации. Скрытие информации может быть пространственным, временным, структурным и энергетическим. Пространственное скрытие достигается размещением источника информации в местах (тайниках), неизвестных злоумышленнику. Временное скрытие обеспечивается путем скрытия времени создания секретной (конфиденциальной) информации (например, времени совещания), времени проявления информативных демаскирующих признаков (например, во время испытаний новой продукции) и (или) предотвращение доступа средства добывания к источникам информации в течение известного времени его работы (например, на время пролета над объектом защиты космического разведывательного аппарата). Структурное скрытие предусматривает изменение демаскирующих признаков объектов защиты под окружающий фон (маскировкой) или подобъект прикрытия (дезинформированием). Структурное скрытие информации, отображаемой с помощью символов семантической информации, называется шифрованием, основы которого рассматриваются криптографией. Энергетическое скрытие основывается на снижении соотношения энергии носителя информации и помех на входе приемника сигналов злоумышленника, при которых качество добываемой информации становится ниже допустимого.

13. Инженерная защита обеспечивается путем применения инженерных конструкций (заборов, дверей, окон, стен, шкафов, хранилищ, сейфов др.) на границах и внутри контролируемых зон для создания механических преград на пути действий злоумышленника и стихийных сил. С целью обнаружения источников угроз и их эффективной нейтрализации широко применяются технические средства охраны. Технические средства охраны включают средства обнаружения, видеоконтроля, тревожного оповещения, нейтрализации угроз и управления. Инженерные конструкции со средствами обнаружения внешних воздействий образуют рубежи защиты. Силы и средства технической охраны объединяются в автономные и централизованные системы. В автономной системе нейтрали-

зация угроз производится силами и средствами самой системы, в централизованной системе для этого привлекаются внешние силы и средства, например, вневедомственной охраны.

14. Для предотвращения утечки акустической информации применяется временное, структурное и энергетическое скрытие. Временное скрытие обеспечивается путем скрытия времени генерации секретной (конфиденциальной) акустической информации. Речевую информацию, передаваемую по каналам связи, защищают путем ее шифрования и структурного скрытия сигналов каналов связи (технического закрытия). Для защиты речевой информации в узкополосных телефонных каналах связи применяют статические (с постоянным ключом в течение сеанса связи) и динамические (с изменяющимся во время сеанса связи ключом) частотные и временные перестановки полос спектра и временных отрезков, а также их комбинации. Стойкость защиты при комплексном использовании этих методов приближается к стратегическому уровню. Стратегическая стойкость речевого сигнала в телефонных каналах связи обеспечивается путем шифрования на передающей стороне информационных медленно меняющихся его параметров (основного тона, моментов изменения тон/сигнал и др.) и синтеза по ним речи на приемной стороне. Эти методы реализуются в средствах, называемых вокодерами.

Энергетическое скрытие акустических сигналов достигается их звукоизоляцией, звукопоглощением и зашумлением. Звукоизоляция обеспечивается ограждениями помещения (стенами, потолком, полом, дверьми, окнами), акустическими экранами, кабинами, кожухами и глушителями. Для звукопоглощения применяются мягкие, полужесткие и жесткие материалы, а также резонансные поглотители звука. Для подавления энергии акустической волны, падающей на нагревательные конструкции (батареи, панели, стены), применяют перфорированные резонаторные поглотители звука. Зашумление достигается излучением в диапазоне частот опасного акустического сигнала акустическим генератором воздушной акустической и виброакустической волны со случайно изменяющейся амплитудой, превышающей уровень опасного сигнала. Для подавления речевого сигнала наиболее эффективен шум с речеподобным спектром, уровень которого должен превышать уровень речевого сигнала в 6–8 раз. Особенностью зашумления рече-

вого сигнала является установка акустического генератора ближе к акустическому приемнику злоумышленника по сравнению с удаленностью источника защищаемой информации.

15. Для предотвращения утечки речевой информации по составному каналу кроме мер по нейтрализации акустического канала принимаются меры по подавлению опасных сигналов в радиоэлектронном и оптическом каналах, последовательно соединенных с акустическим каналом. Закладные устройства как источники сигналов радиоэлектронного канала составного акусто-радиоэлектронного канала утечки информации обнаруживаются по их демаскирующим признакам: конструкции (проводу — антенне, отверстию перед микрофоном, химическим источникам тока внутри устройства и др.), радиоизлучениям, наличию в устройстве полупроводниковых и металлических элементов, изображению электрической схемы при просвечивании рентгеновскими лучами и др.

Утечка информации в оптическом канале составного акусто-оптического канала предотвращается путем экранирования акустического сигнала шторами на окнах и вибро-акустическим зашумлением их стекол.

16. Противодействие наблюдению путем пространственного скрытия объектов наблюдения производится путем расположения их в местах, недоступных несанкционированному наблюдению. Структурное скрытие объектов наблюдения достигается маскировкой и дезинформированием наблюдателя. Маскировка обеспечивается изменением видовых демаскирующих признаков объекта защиты под признаки окружающих его объектов (фона). Она производится путем маскировочного окрашивания объектов, применением естественных и искусственных масок. Для дезинформирования объект окрашивают под объект прикрытия или применяют деформирующие искусственные маски с признаками объекта прикрытия. В радиодиапазоне для структурного скрытия применяют также переотражатели электромагнитной волны с большой эффективной площадью рассеяния (уголковые и линзовые отражатели, дипольные отражатели и другие конструкции).

Энергетическое скрытие объектов наблюдения в оптическом диапазоне обеспечивается уменьшением яркости объекта, ухудшением прозрачности среды распространения аэрозолями, за-

светкой изображения объекта на светочувствительном экране оптического приемника и ослеплением оптического приемника. При ослеплении нарушается рабочий режим светочувствительных элементов приемника, в результате чего искажается электронное изображение при преобразовании света в электрический сигнал. В радиодиапазоне для энергетического скрытия уменьшают эффективную площадь рассеяния путем устранения «блестящих точек» на поверхности защищаемого объекта, покрытия ее материалами, поглощающими электромагнитные волны, а также генерацией помех.

17. Для противодействия добыванию информации путем перехвата содержащих ее радио- и электрических сигналов применяются все виды скрытия как информации, так и сигналов. Пространственное скрытие обеспечивается сохранением в тайне местонахождения источника излучения и его частот, увеличением коэффициента направленного действия его антенны, устранением побочных излучений ОТСС. Структурное скрытие реализуется в виде структурного скрытия информации и сигналов. Структурное скрытие информации в символьной форме (при цифровой передаче) достигается шифрованием. Для скрытия сигналов используются методы технического закрытия, псевдослучайные сигналы и сигналы со скачкообразным изменением частоты, которые не принимаются типовыми радиоприемниками. Уменьшение до допустимых значений опасных электрических сигналов при реализации энергетического скрытия достигается их подавлением. Методы и способы подавления зависят от демаскирующих признаков опасных сигналов. Если таковым признаком является частота, то применяется фильтрация опасного сигнала, если амплитуда, то его ограничение, если направление распространения опасных сигналов, то используются однонаправленные согласующие устройства (эмиттерные повторители). Побочные электромагнитные излучения ослабляются путем экранирования узлов, устройств, проводов.

Энергетическое скрытие опасных сигналов производится также путем пространственного и линейного зашумления опасных сигналов. Пространственное зашумление заградительной помехой эффективно для подавления излучений ПЭМИН. Но для подавле-

ния опасных радиосигналов большей мощности необходимы прицельные помехи. Для защиты речевой информации в телефонных линиях путем линейного зашумления используются помехи в звуковом и ультразвуковом диапазонах частот. Частота помехи в ультразвуковом диапазоне близка к верхней частоте звукового диапазона. Такая помеха, не искажая передаваемый по телефонной линии речевой сигнал, проникает через входные селективные цепи закладного устройства и нарушает его нормальный режим работы. В результате этого в закладном устройстве возникают нелинейные искажения, исключающие подслушивание.

## Литература к разделу II


1. Федеральный закон «Об информации, информатизации и защите информации». Принят Государственной Думой 25 января 1995 года.
2. *Ожегов С. И.* Словарь русского языка. — М.: Советская энциклопедия, 1968.
3. Философский словарь / Под ред. *И. Т. Фролова.* — М.: Издательство политической литературы, 1991.
4. Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне».
5. *Ярочкин В. И., Шевцова Т. А.* Словарь терминов и определений по безопасности информации. — М.: Ось-89, 1996.
6. Радиолокационные станции воздушной разведки / Под ред. *Г. С. Кондратенкова.* — М.: Воениздат, 1983.
7. *Варламов А. В., Кисиленко Г. А., Хореев А. А., Федоринов А. Н.* Технические средства видовой разведки / Под ред. *А. А. Хорева.* — М.: Москва, РВСН, 1997.
8. *Харкевич А. А.* Спектры и анализ. — М.: Государственное издательство физико-математической литературы, 1962.
9. *Плэтт В.* Стратегическая разведка. Основные принципы. — М.: Форум, 1997.
10. *Харкевич А. А.* Теоретические основы радиосвязи. — М.: Государственное издательство технико-теоретической литературы, 1957.
11. *Кученков Е. Б.* Каналы возможной утечки информации за счет вспомогательных технических средств и систем // Вопросы защиты информации. — 1999. — № 3. — С. 46–53.
12. *Волгин М. Л.* Паразитные связи и наводки. — М.: Советское радио, 1965.

13. *Шеннон К.* Математическая теория связи. Работы по теории информации и кибернетике. — М.: Издательство иностранной литературы, 1963.
14. Съем информации по виброакустическому каналу. Подготовлен экспертной группой компании «Гротек» // Системы безопасности связи и телекоммуникаций. — 1995. — № 5. — С. 12–14.
15. *Хорев А. А., Макаров Ю. К.* К оценке эффективности защиты акустической (речевой) информации // Специальная техника. — 2000. — № 5. — С. 46–56.
16. *Волобуев С. В.* Безопасность социологических систем. — Обнинск: Викиинг, 2000.
17. *Николаенко Ю. С.* Противодействие радиотехнической разведке // Системы безопасности связи и телекоммуникаций. — 1995. — № 6. — С. 12–15.
18. *Яглом А. М., Яглом И. М.* Вероятность и информация. — М.: Наука, 1973.
19. Акустика: Справочник под общей редакцией *М. А. Сапожкова.* — М.: Радио и связь, 1989.
20. *Андрианов В. И., Соколов А. В.* «Шпионские штучки 2» или как сберечь свои секреты. — СПб.: Полигон, 1997.
21. *Свечков Л. М., Чурляев Ю. А.* Защита коммерческой тайны в производственно-предпринимательской деятельности. — М.: Центральный институт повышения квалификации кадров авиационной промышленности, 1992.
22. ГОСТ Р 50862-96. Сейфы и хранилища ценностей. Требования и методы испытаний и огнестойкость. — М.: Госстандарт России, 1996.
23. *Белоусов Е. Ф., Гордин Г. Т., Ульянов В. Ф.* Основы систем безопасности объектов. Часть 1. Введение в системы охранной безопасности: Учебное пособие / Под ред. *Ю. А. Оленина.* — Пенза: Изд-во Пензенского гос. ун-та, 2000.
24. *Арлащенков Ю. П., Ковалев М. С., Котов Н. Н., Тюрин Е. П.* Применение технических средств в борьбе с терроризмом. — М.: НИЦ «Охрана» ГУВО МВД России, 2000.
25. *Барсуков В. С., Дворянкин С. В., Шеремет И. А.* Безопасность связи в каналах телекоммуникаций. Серия «Технология электронных коммуникаций», т. 20. — М.: НИФ «Электронные знания»; СП «Эко-Трендз», 1992.
26. *Семенов Д. В., Ткачев Д. В.* Нелинейная локация: концепция NR // Специальная техника. — 1999. — № 1–2. — С. 17–22.

27. *Скребнев В. И.* Подповерхностная локация: новые возможности // Специальная техника. — 1998. — № 1. — С. 9–10.
28. *Котенев А. А., Лекарев С. В.* Современный энциклопедический словарь по безопасности. Секьюрити. — М.: Ягуар, 2001.
29. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Решение Коллегии Гостехкомиссии России № 7.2/02.03.2001 г.

27 Зак. 174

# Раздел III. Технические основы добывания и инженерно-технической защиты информации

Рассмотренные во втором разделе теоретические основы добывания и защиты информации реализуются людьми и техническими средствами. Силы и средства, обеспечивающие достижение поставленных целей и решение задач, образуют системы технической разведки и инженерно-технической защиты информации.

## Глава 14. Характеристика средств технической разведки

### 14.1. Структура системы технической разведки

Органы разведки образуют систему разведки с многоуровневой иерархической структурой, приведенной на рис. 14.1.

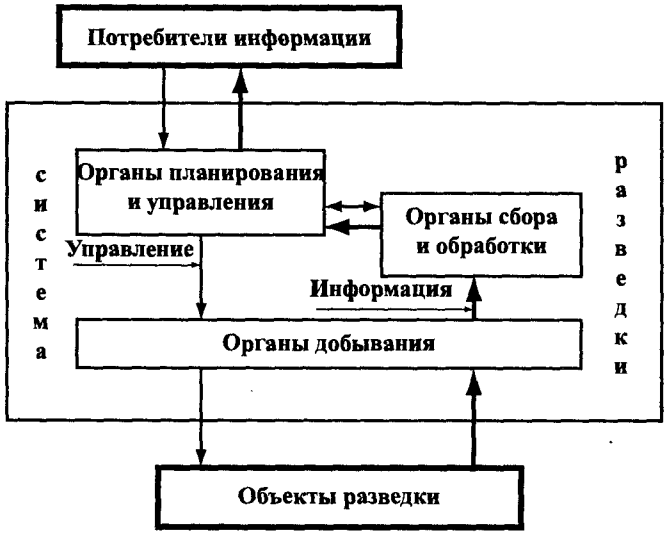



*Рис. 14.1.* Структура системы разведки

Тонкими линиями на этом рисунке показаны пути передачи команд управления, толстыми — передачи добытой информации. Совместно они образуют контуры циклов разведки. Как следует из рисунка, таких циклов может быть несколько: **полный** и **локальные** циклы. Полный цикл охватывает органы разведки и потребителей разведывательной информации: потребители информации — органы планирования и управления — органы добывания — объекты разведки — органы добывания — органы сбора и обработки — органы планирования и управления — потребители информации. Кроме него возникает необходимость в локальных циклах между различными органами системы разведки: органами управления и обработки, обработки и добывания. Например, при разработке плана разведывательной операции используется информация, накопившаяся в органе сбора и обработки. В ходе обработки новой информации может возникнуть необходимость в дополнительной разведке (доразведке) отдельных объектов или их действий.

Органы планирования и управления преобразуют задачи потребителей информации в планы проведения разведывательной операции и команды управления исполнителям. Планы и команды передаются как в органы сбора и обработки, так в органы добывания. Органы сбора и обработки собирают данные и сведения от органов добывания и в случае их противоречивости или недостаточности для принятия решения подают команду на доразведку. После получения ответов на поставленные потребителями информации вопросы органы информационной работы готовят информационные материалы, которые через руководство системы разведки передаются или докладываются потребителям информации.

Схеме на рис. 14.1 далеко не всегда соответствует административная структура органов разведки, в особенности разведки в интересах коммерческих структур — коммерческой разведки. Необходимость указанных на рисунке уровней обусловлена объективными процессами добывания информации. В минимальном варианте функции системы добывания информации могут быть реализованы одним или несколькими работниками службы безопасности малочисленной фирмы.

За свою историю разведка накопила большой опыт по добыванию информации, в том числе с использованием технических

средств. Задачи по добыванию информации инициируют исследования по созданию принципиально новых способов и технических средств разведки. С этой целью органы разведки ведущих стран имеют мощную научно-производственную базу.

## 14.2. Классификация технических средств добывания информации

Еще недавно, каких-то 100–150 лет тому назад, добывание информации осуществлялось в основном с помощью органов чувств человека. Научно-технический прогресс в XIX и особенно в XX веках резко изменил ситуацию. В настоящее время подавляющая часть информации добывается с помощью технических средств.

Технические средства существенно расширяют и дополняют возможности человека по добыванию информации, обеспечивая:

- съем информации с носителей, которые недоступны органам чувств человека;
- добывание информации без нарушения границ контролируемой зоны;
- передачу информации практически в реальном масштабе времени в любую точку земного шара;
- анализ и обработку информации в объеме и за время, недостижимых человеком;
- консервацию и сколь угодно долгое хранение добываемой информации.

Классификация технических средств добывания информации по их назначению приведена на рис. 14.2.

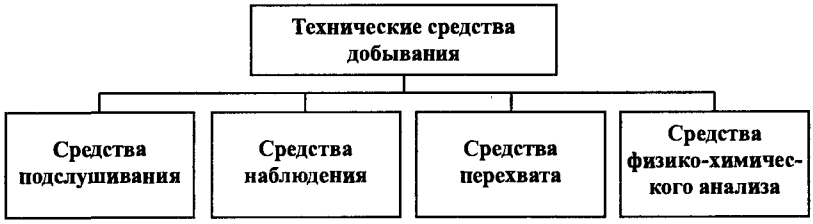



*Рис. 14.2.* Классификация средств добывания информации по назначению

Граница между видами средств добывания достаточно условная. Условность объясняется неоднозначностью и пересечением понятий «подслушивание», «наблюдение» и «перехват». Подслушивание предполагает несанкционированное добывание акустической информации путем как восприятия акустических сигналов непосредственно ушами или с помощью акустического приемника, так и в результате промежуточной ее ретрансляции. Несанкционированное подслушивание телефонного разговора абонентов сотовой связи осуществляется путем перехвата сигналов соответствующей линии связи. Аналогичная неоднозначность возникает при наблюдении. Наряду с непосредственным наблюдением с помощью визуально-оптических приборов или приборов ночного видения возможно дистанционное наблюдение с помощью телевизионной камеры на летательном аппарате (космическом аппарате, пилотируемом самолете, беспилотном самолете-разведчике), радиосигнал которой может быть в принципе передан на любое расстояние. Одним из способов скрытого наблюдения за объектом разведки может быть получение его изображения в результате перехвата из функционального канала связи телевизионного сигнала. Но «перехват» — способ добывания информации из радиоэлектронного канала. Учитывая эту неоднозначность, в дальнейшем под **подслушиванием** и **наблюдением** будем понимать добывание информации из простых акустических и оптических каналов ее утечки. Добывание информации из составных каналов утечки рассматривается как **дистанционное подслушивание** и **наблюдение**, одним из этапов которых может быть перехват сигналов с представляющей интерес информацией.

Так как дальность непосредственного (только ушами) подслушивания мала и оно связано с большим риском для злоумышленника, то создание технических средств подслушивания направлено, прежде всего, на увеличение длины акустического канала утечки речевой информации. Технические средства подслушивания позволяют также снимать информацию с носителей, распространяющихся в воде и твердой среде на значительно большее расстояние, чем в воздухе. Запись акустических сигналов существенно повысила объективность добываемой акустической информации и позволила осуществлять подслушивание автономно (без непосредственного участия человека).

Хотя зрительная система человека имеет достаточно высокие показатели, но приспособлена для обеспечения жизни человека, а не для скрытного наблюдения в условиях, малопригодных для обеспечения жизнедеятельности. Риск злоумышленника при наблюдении минимален, когда он находится вне поля зрения сотрудников службы безопасности. Технические средства наблюдения существенно расширяют возможности зрения человека по диапазону длин волн, дальности и чувствительности. Наблюдения в инфракрасном и радиодиапазонах увеличивают информативность признаковых структур объектов разведки, что способствует повышению вероятности их обнаружения и распознавания. Но мало людей имеют так называемую «фотографическую» память, демонстрируемую советским разведчиком в фильме «Щит и меч». Большинство людей не могут не только воспроизвести текст на десятках страниц после кратковременного просмотра, но даже рассказать близко к тексту их содержание. Причем человек при воспроизведении изображения может его существенно исказить, как делают это, например, свидетели происшествия или преступления. Так как изображение содержит большой объем информации, то для ее добывания крайне важно законсервировать изображение для последующего детального анализа.

Средства перехвата обеспечивают несанкционированный прием радио- и электрических сигналов и радиоактивных излучений, недоступных органам чувств человека. Так как органы чувств человека не участвуют в перехвате, то соответствующие технические средства выполняют полный набор функций по снятию информации радио- и электрических сигналов, а также потока радиоактивных частиц: обнаружение, прием, преобразование, усиление, регистрация, хранение, анализ и, наконец, преобразование электрических сигналов в вид, доступный органам чувств человека.

Если носителями информации являются макротела, добыванием информации на этих носителях занимается злоумышленник, который их похищает или собирает в местах, куда носители в виде отходов выбрасываются. Вещественные признаки добываются в результате физического и химического анализа проб твердых, жидких и газообразных веществ, добытых с мест их сброса.

Технические средства добывания в зависимости от места установки и условий эксплуатации имеют различные схемотехнические и конструктивные решения. Условия эксплуатации (климатические воздействия, механические нагрузки, требования к масса-габаритным характеристикам) весьма существенно сказываются на возможностях технических средств добывания информации.

К средствам технической разведки, размещаемым на воздушных и космических носителях, предъявляются жесткие требования к масса-габаритным характеристикам, энергопотреблению, устойчивости к механическим воздействиям (перегрузкам и вибрациям). Требования к аппаратуре по электрическим и масса-габаритным характеристикам противоречивы: улучшение электрических параметров приводит к усложнению схемотехнических решений, увеличению масса-габаритных характеристик и энергопотреблению. Например, повышение производительности процессора компьютера создало проблему его охлаждения, решение которой сопровождается увеличением размеров и массы вентиляторов.

Улучшение параметров на каждом этапе развития радиоэлектроники, оптики и других прикладных областей науки и техники достигается усложнением аппаратуры до тех пор, пока не реализуются новые идеи, приводящие к скачку в методах и технологии. Но на определенном этапе технического прогресса усложнение технических решений приводит к увеличению веса и габаритов средств добывания.

Противоречие разрешается путем дифференцированного применения средств добывания. Классификация средств добывания информации по условиям эксплуатации приведена на рис. 14.3.

**Стационарная аппаратура** размещается в отапливаемых в зимнее время помещениях и неотапливаемых местах. К ней предъявляются требования по устойчивости к механическим и климатическим воздействиям (вибрациям, ударам, температуре, влажности), пониженные по сравнению с требованиями к мобильной аппаратуре. За счет облегченных требований к условиям эксплуатации в этой аппаратуре при приемлемых (обеспечивающих перевозку в упакованном виде) весе, габаритах и энергопотреблении реализуются в полном объеме достижения в соответствующих областях науки и техники. Естественно, к аппаратуре, работающей в

неотапливаемых местах, предъявляются существенно более жесткие требования по климатическим условиям, которые реализуются за счет использования холодоустойчивых элементов или их дополнительного подогрева.

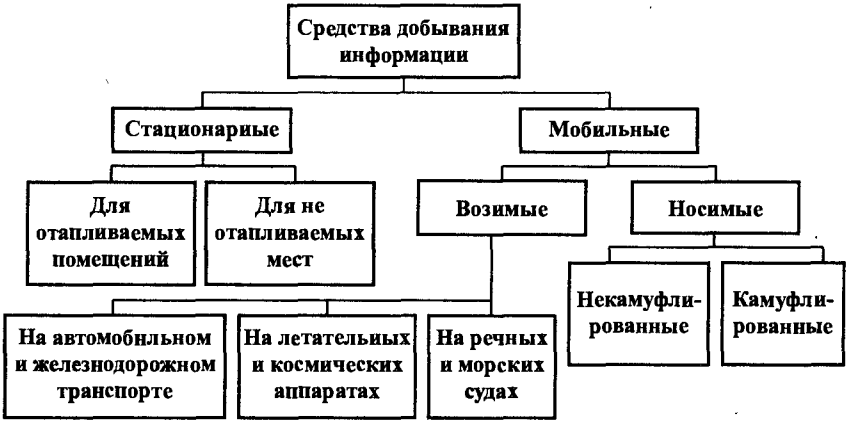



*Рис. 14.3.* Классификация средств добывания по условиям эксплуатации

Такая, в основном радиоэлектронная, аппаратура устанавливается в посольствах и консульствах зарубежных государств для добывания информации с территории посольства или консульства, рассматриваемых по международному праву как территория соответствующего государства. Однако она может быть размещена в иных, неотапливаемых местах, вблизи источников опасных сигналов, например возле военных аэродромов и полигонов. Радиоэлектронные устройства в автономном режиме, без участия человека, ретранслируют или записывают перехваченные электрические и радиосигналы с последующей ускоренной передачей накопленной информацией или изъятия пленки магнитофона злоумышленником. Например, американские специалисты создали средства «Камбала» и «Крот» для съема информации с бронированных кабельных линий связи, размещаемых под водой и в земле. Средство «Камбала» представляет собой сложный радиоэлектронный комплекс, размещаемый в стальном герметичном цилиндре длиной более 5 м и диаметром 1,2 м. Информация с кабеля снимается с помощью индукционных датчиков с захватами. После уси-

ления и обработки сигналы записываются на 60 магнитофонов (в «Камбале») и на магнитный диск специального 60-канального магнитофона (в «Кроте») с продолжительностью непрерывной записи на каждом магнитофоне и в каждом канале 150 часов и 115 часов соответственно. Включение и выключение записи производится по уровню перехватываемого сигнала. После окончания пленки или заполнения диска радиомаяки передают (в «Камбале» через буй) соответствующие сигналы, в том числе об отсутствии внешних воздействий на эти устройства. Кроме того, эти средства минируются на неизвлекаемость. Для обеспечения работоспособности в течение десятков лет средство «Камбала» оснащается ядерным (плутониевым) источником электропитания. Это средство было обнаружено при ремонте подводной кабельной линии Магадан–Хайрузово в Охотском море.

В принципе стационарная аппаратура может быть также установлена в помещении жилого дома вблизи фирмы конкурента. Однако задачи по добыванию информации проще решаются с помощью мобильной аппаратуры.

**Мобильная аппаратура** широко применяется органами добывания как зарубежного государства, так и коммерческих структур. К ней предъявляются более жесткие требования по размещению и функционированию в стоящем или даже движущемся автомобиле, на борту летательного аппарата, космического аппарата или морского судна. Наиболее жесткие требования по виброустойчивости предъявляются к средствам добывания информации, размещаемым на воздушных и морских судах. Поэтому эти средства имеют прочные корпуса и крепления.

Существующая **возимая** на автомобилях аппаратура обеспечивает визуально-оптическое и телевизионное наблюдение, фотографирование, перехват радиосигналов, подслушивание с использованием закладных устройств. Например, размещаемый в автомобильной антенне эндоскоп HR 1780-S позволяет скрытно вести наблюдение из автомобиля. Те же задачи решает видеокамера PK 5045 с оптикой, вмонтированной в антенну. Вращая антенну из салона автомобиля, можно на экране телевизионного приемника в нем наблюдать и записывать на видеомагнитофон изображение субъектов и объектов вокруг машины.

Большие возможности обеспечивает возимая автоматическая аппаратура, которая записывает подслушанные звуковые сигналы и перехваченные радиосигналы в отсутствие в машине человека-оператора. В этом случае припаркованный возле фирмы автомобиль может находиться длительное время, не вызывая подозрение у ее службы безопасности.

**Носимая** некамуфлированная портативная аппаратура размещается в одежде человека, сумках, портфелях. Например, при посещении офиса банка или другой коммерческой структуры можно положить небольшую сумку с вмонтированной в нее теле- или кинокамерой на стол и в поле ее зрения попадут изображения на экранах компьютеров сотрудников, работающих за другими столами.

Средства добывания, камуфлированные под различные бытовые приборы и предметы личного пользования, могут быть максимально приближены к источникам информации, но технические параметры камуфлированных средств добывания обычно хуже аналогичных параметров некамуфлированных средств.

Носимая аппаратура добывания используется непосредственно злоумышленником или после установки работает в автономном режиме. В литературе упоминаются различные виды портативных автономных технических средств: закладные подслушивающие устройства в помещениях, автономные портативные технические средства разведки на местности, портативные средства наблюдения, устройства слежения за транспортными средствами. Всех их объединяют общие свойства — автономный или дистанционно управляемые режимы работы по добыванию информации, скрытная установка в пределах досягаемости носителя добываемой информации. Поэтому их можно объединить общим понятием — **закладные устройства**. Хотя закладные устройства создают реальную угрозу безопасности злоумышленника в момент их установки и изъятия, они все шире применяются для негласного добывания информации.

По физической природе носителя добываемой информации закладные устройства можно разделить на **акустические, оптические, радиоэлектронные, радиационные**.

Акустические закладные устройства воспринимают акустические сигналы в воздухе, твердых телах и воде соответственно и преобразуют их в электрические сигналы. Эти сигналы после

усиления и возможного сдвига по частоте могут передаваться по электрическим проводам или светопроводам, модулировать колебания радиопередающих устройств или записываться на магнитной ленте или тонкой проволоке из ферромагнитного материала. Акустические закладные устройства, воспринимающие колебания земной поверхности, называются **сейсмическими**. Они широко применялись и применяются в Афганистане и в иных горячих точках для дистанционного обнаружения на удалении до единиц км движущихся людей и техники и передачи по радиоканалу сигналов оповещения и координат объектов поражения.

Оптические закладные устройства представляют собой автоматически или дистанционно управляемые фотоаппараты или телевизионные камеры. Традиционные пленочные фотоаппараты обеспечивают пока более высокое разрешение изображения, чем цифровые, могут иметь очень малые размеры, например размещаться в наручных часах, зажигалке и других предметах личного пользования, но требуют физического изъятия и химической обработки фотопленки. Последнее обстоятельство важно с точки зрения оперативного использования оптического закладного устройства. Преобразование оптического изображения в электрические сигналы в цифровых фотоаппаратах и телевизионных камерах (видеокамерах) позволяет дистанционно передавать изображения в реальном масштабе времени или записывать изображение на магнитном носителе с последующей ускоренной передачей. Микровидеокамеры встраиваются в картины, настенные часы, скоросшиватели, в сумки и кейсы, в пояс, в автомобильные антенны и другие предметы.

Для обнаружения мест складирования ядерных боеприпасов и стоянок железнодорожных ракетных комплексов применяют закладные устройства, содержащие дозиметры и устанавливаемые в контейнерах, перевозимых железнодорожным транспортом.

## 14.3. Возможности средств технической разведки

Возможности технической разведки и ее средств являются одними из основных факторов, определяющих угрозу безопасности информации. Поэтому органы, обеспечивающие ее безопасность, внимательно отслеживают все изменения и тенденции в развитии

способов и технических характеристик средств добывания информации. Наибольшее влияние на эффективность добывания информации оказывают **диапазон частот воспринимаемых средствами частот сигналов, чувствительность, и разрешающая способность технического средства и его масса-габаритные характеристики**.

**Диапазон частот** носителей информации — сигналов является одним из важнейших их признаков, позволяющих обнаруживать носители с защищаемой информацией. Человек воспринимает световые сигналы в очень узком диапазоне видимого света и акустических сигналов в звуковом диапазоне. Сигналы с иными частотами органам чувств человека недоступны. Поэтому чем шире диапазон частот средства добывания, тем большие его возможности по поиску и обнаружению носителей с защищаемой информацией.

**Чувствительность** технического средства наряду с мощностью источника сигнала и затуханием среды определяют важнейший показатель эффективности разведки — **дальность добывания информации**. А дальность, в свою очередь, влияет на безопасность органа добывания. Чем выше чувствительность средства, тем на большем удалении от источника информации оно обнаруживает и распознает ее носитель. Так как в принципе любое радиоэлектронное средство или электрический прибор создает побочные электромагнитные излучения и наводки, то повышение чувствительности средств добывания расширяет также круг потенциальных источников опасных сигналов. Парадокс развития средств добывания заключается в том, что паразитные излучения и наводки одновременно тормозят рост чувствительности. Для большинства приемников сигналов их предельная чувствительность ограничивается собственными (тепловыми) шумами или внешними помехами. Однако из этого не следует, что в перспективе невозможны качественные изменения в повышении чувствительности приемников сигналов технической разведки. Оптимизм в этом вопросе подкрепляется многими примерами обеспечения чувствительности субъектов живой природы. Например, пока наиболее эффективный поиск наркотиков, взрывчатых веществ, людей под завалами обеспечивают собаки.

**Разрешающая способность** технического средства определяет количество и информативность добываемых с его помощью

признаков объектов разведки. Чем выше разрешающая способность и точность измерения, тем большее количество информативных признаков будет добыто. Например, чем большее количество деталей образца военной техники можно рассмотреть на его фотографии и чем выше точность их измерения, тем больше достоверной информации о тактико-технических характеристиках образца военной техники сможет получить эксперт.

Количество добываемых видовых признаков объекта наблюдения определяется размерами его изображения на сетчатке глаза или мишени (в кадре пленки) фотоприемника и его разрешающей способности. Требования по разрешающей способности на местности, необходимой для обнаружения объекта военной техники и его распознавания (определения типа, описания и анализа), представлены в табл. 14.1 [1].

*Таблица 14.1*

| *Вид объекта* | *Разрешение в м на местности для* | | | |
|---|---|---|---|---|
| | *обнаружения объекта* | *определения типа объекта* | *описания объекта* | *технического анализа* |
| Транспортные средства | 1,5 | 0,6 | 0,06 | 0,045 |
| РЛС | 3,0 | 1,0 | 0,15 | 0,015 |
| Самолеты | 4,5 | 1,5 | 0,15 | 0,045 |
| Ракетные базы | 3,9 | 1,5 | 0,30 | 0,045 |

Если для обнаружения объекта достаточны крупногабаритные видовые признаки (размеры объекта, его конфигурация и др.), то для распознавания типа объекта наблюдения требуются более мелкие признаки, а для описания объекта и его технического анализа необходимо наблюдать мелкие детали конструкции и особенности поверхности. Поэтому, как следует из табл. 14.1, разрешение, необходимое для определения типа объекта, в несколько раз выше, чем для обнаружения, а для получения признаков, на основе которых возможно описание и технический анализ, разрешение должно быть в десяти раз выше.

Возможности наблюдения тем выше, чем больше фокусное расстояние и разрешение оптического приемника. Но при увеличении f обратно пропорционально уменьшается угол зрения опти-

ческого прибора и существенно усложняется поиск объекта наблюдения. При уменьшении угла зрения прибора в 2 раза время поиска (просмотра одинаковой части пространства) увеличивается в 4 раза. Поэтому в оптической разведке используют два режима: **обзорный и детальный.**

Обзорное наблюдение проводится с целью обнаружения объекта разведки, детальное — для его распознавания. Для реализации такой возможности в современных биноклях используются оптические системы с переменным фокусным расстоянием, у которых кратность увеличения может изменяться в широких пределах (от 4 до 20 и более). При изменении кратности увеличения в обратно пропорциональной зависимости изменяется угол зрения. Такие бинокли при большом угле зрения позволяют наблюдать большую часть пространства, а после обнаружения объекта рассматривать его при большем увеличении. Для наблюдения объектов под очень малыми углами зрения (несколько градусов) современные перспективные приборы имеют устройство стабилизации поля зрения. Без него при незаметных на глаз колебаниях (треморе) рук изображение объекта наблюдения может выходить за пределы поля зрения. А специальные телескопы для наблюдения за объектами на удалении до 10 км устанавливаются на стационарных платформах и штативах.

Тесная связь существует между разрешающей способностью средства добывания и информативностью добываемых сигнальных и вещественных признаков. Например, так как практически очень сложно сделать одинаковыми частоты задающих генераторов радиоизлучающих средств одного и того же типа, то при высоком разрешении измерителя частоты возможно по этому признаку различать передатчики одного и того же типа.

Но так как количество и качество добываемой информации в общем случае уменьшаются с увеличением дальности добывания, то в разведке существует проблема обеспечения доступа средства разведки к источникам информации без существенного увеличения риска для ее органов. Возможности доступа средств разведки существенно зависят от массы и габаритов. Чем они меньше, тем проще приблизить его к источнику информации и обеспечить условия разведовательного контакта. Риск минимален, если средс-

тво добывания находится вне контролируемой зоны. Для обеспечения дистанционного доступа к объектам разведки ее технические средства размещаются на земле (на местности, в зданиях, на наземном транспорте), воздушных летательных аппаратах, космических аппаратах, на речных и морских судах.

В мирное время наиболее близкий доступ к любым объектам на поверхности земли и воды обеспечивает **космическая разведка**. Параметры траектория движения КА (высота орбиты, угол ее наклонения относительно экватора Земли) со средствами разведки на борту определяются направлением и скоростью вывода ракеты-носителя. Для вывода КА на околоземную орбиту ему нужно при запуске сообщить первую космическую скорость у поверхности Земли не менее 7,91 км/с. При этой скорости орбита КА круговая. Минимальная высота ограничена тормозящим действием остатков атмосферы и составляет 130–150 км. Чем выше скорость, тем больше высота орбиты. При второй космической скорости более 11,186 км/с КА может выйти из сферы действия тяготения Земли.

В зависимости от скорости и направления выведения КА располагаются на низких круговых, высоких эллиптических, геостационарных орбитах (см. рис. 14.4).

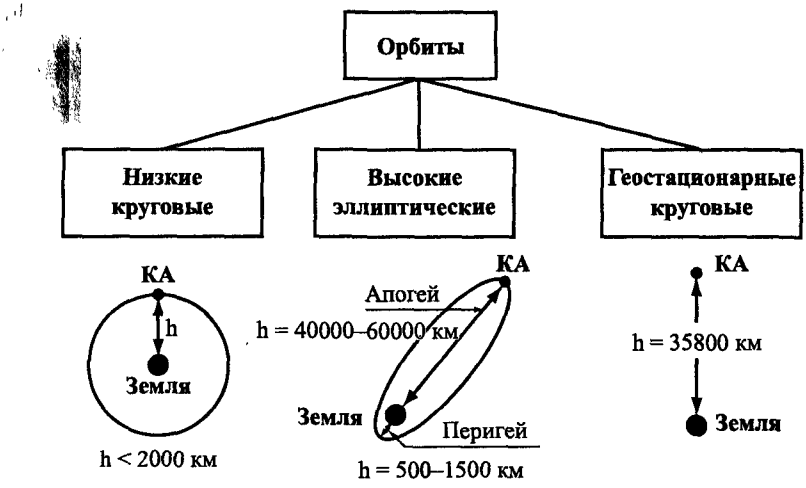



*Рис. 14.4.* Виды орбит КА

**Низкие круговые орбиты** — наиболее распространенные орбиты разведывательных КА, так как они позволяют им приблизиться к объекту на минимально допустимое расстояние. От этого расстояния зависит время нахождения («жизни») КА. С уменьшением высоты орбиты увеличивается торможение КА остатками атмосферы и сокращается время его существования на орбите. Противоречие между временем пребывания на орбите низколетящего КА и стремлением приблизить средства добывания информации к ее источникам решается путем создания маневрирующих спутников. Например, разведывательный КА фотографической разведки США Keyhole-11A может маневрировать на орбите по заданной программе или команде с Земли: он снижается до высоты 130–160 км, производит детальную фотосъемку в видимом и ближнем ИК-диапазонах с разрешением до 10 см, после чего поднимается на большую высоту (до 1000 км), ведя с нее обзорное наблюдение. Передача информации на наземный пункт приема производится по радиоканалу непосредственно или через спутник-ретранслятор.

Однако низкоорбитальные КА, пролетая с большой скоростью над поверхностью Земли, позволяют наблюдать объект или осуществлять перехват его радиосигналов в течение очень короткого времени (единиц минут). Период вращения КА вокруг Земли $T_{ка}$ в минутах в зависимости от высоты орбиты h можно оценить по формуле:

$$T_{ка} \approx T_0(1 + h / R_з)^{3/2},$$

где $R_з = 6372$ км — радиус Земли; $T_0 = 84{,}4$ мин. — период обращения гипотетического КА по круговой орбите с радиусом, равным радиусу Земли ($h = 0$).

В табл. 14.2 приведены некоторые значения $T_{ка}$, рассчитанные по этой формуле.

*Таблица 14.2*

| h, км | 100 | 200 | 300 | 400 | 500 | 1000 | 5000 | 10000 | 35870 | 50000 | 100000 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_{ка}$, мин. | 86,4 | 88,4 | 90,4 | 92,5 | 94,5 | 105 | 201,2 | 349 | 1440 (24 ч) | 2231 | 5784 |

Из этой таблицы видно, что на малых высотах период вращения КА равен приблизительно 1,5 часа. Однако из этого не следует, что КА будет находиться над одним и тем же районом через каждые 1,5 часа. Из-за вращения Земли вокруг оси на каждом очередном витке КА будет пролетать над новым районом Земли и только через сутки ситуация повторится.

Возможности просмотра различных районов Земли зависят от угла наклона плоскости орбиты КА относительно плоскости экватора Земли. Если КА расположен на **круговой полярной орбите**, то его средства могут периодически просматривать всю поверхность Земли. Например, одновременная работа 2 спутников (с высотой орбит 1000–1400 км и наклонениями, близкими к 90°) позволяет просматривать район земного шара с интервалом в 6 ч. КА на **солнечно-синхронной** орбите (с наклонением приблизительно 97°) пролетает над объектом в одно и то же время суток, например днем. С повышением высоты орбиты, как следует из таблицы, период вращения КА увеличивается и при h около 36 тыс. км он равен периоду вращения Земли.

Когда плоскости орбиты КА на высоте около 36 тыс. км и экватора Земли совпадают ($i = 0°$), то КА расположен на **геосинхронной орбите** и постоянно «висит» над одним и тем же районом Земли. Будучи расположенными в плоскости экватора Земли, средства добывания КА не «видят» из-за кривизны Земли ее северные (более 70 градусов широты) районы. Это обстоятельство и большая удаленность КА от поверхности Земли существенно ограничивают возможности геостационарных спутников наблюдением ярких источников света (например, факелов ракет при пуске) и перехватом достаточно мощных радиосигналов.

Промежуточное положение занимают КА на **высоких эллиптических орбитах** (см. рис. 14.4). Системы космической связи на эллиптических орбитах позволяют осуществлять радио- и телевизионное вещание на всей территории России. Типовая орбита соответствует эллипсу с перигеем (наименьшим расстоянием до поверхности Земли — 400–460 км) и апогеем (наибольшим расстоянием — до 60000 км).

Для добывания информации на КА устанавливаются различные средства добывания (фото-, телевизионного и радиоло-

кационного наблюдения, радио- и радиотехнической разведки). Аппаратура современных разведывательных низкоорбитальных КА обладает высокими возможностями. Наибольшее разрешение обеспечивают КА фоторазведки. Установка на КА аппаратуры обзорной разведки позволяет производить съемку поверхности Земли в полосе шириной до 180 км при линейном разрешении на местности 2,5–3,5 м. Опознаются объекты размером 12,5–35 м. Детальная фоторазведка обеспечивает полосу съемки шириной 12–20 км, разрешение на местности 0,3–0,6 м (для маневрирующих — до 0,1 м) и опознавание объектов размером 1,5–6 м.

Космическая разведка США имеет на вооружении разнообразные разведывательные системы: специализированные (фото-, оптико-электронные, радио- и радиотехнические, радиолокационные) и комплексной разведки, например, фотографирование и перехват радиотехнических сигналов. По мере прогресса в миниатюризации средств добывания доля комплексных систем возрастает. При наблюдении за наземными объектами из космоса разрешение аэрофотоаппаратов, установленных на КА, ограничивается не только разрешением объективов и фотопленки или иных светочувствительных элементов, но и турбулентностью атмосферы, Атмосфера представляет собой неоднородную среду распространения света, различные области которой имеют динамически изменяющуюся плотность воздуха и, следовательно, разные оптические свойства, в том числе и коэффициент преломления. Изменение оптических свойств атмосферы во время экспозиции приводит к размыванию границ деталей изображения. В результате этого разрешение фотоаппаратов КА из-за турбулентности атмосферы составляет около 8 см. Компенсация искажений среды в принципе возможна с помощью адаптивной оптики, способной изменять кривизну поверхности линзы или зеркала в соответствии с изменением оптических свойств среды распространения.

Таким образом, космическая разведка обеспечивает наиболее близкий и безопасный для органа добывания доступ к защищаемым объектам и в силу этого обладает достаточно высокими показателями по разрешению и достоверности получаемой информации.

В то же время космическая разведка имеет ряд особенностей, которые облегчают задачу защиты информации на объекте. Кратковременность нахождения низкоорбитального КА над защищаемыми объектами, возможность точного расчета характеристик орбит и моментов времени пролета спутников над защищаемыми объектами позволяют применять простые, но эффективные меры по защите информации. Эти меры противодействуют, прежде всего, выполнению временного условия разведывательного контакта — возможности наблюдения за объектом в момент пролета КА над ним.

Средства добывания размещаются также на летательных аппаратах (самолетах-разведчиках, беспилотных летательных аппаратах) и кораблях, летающих и плавающих вдоль воздушной и морской границ.

С целью увеличения дальности видимости с самолетов-разведчиков соответствующей конструкцией добиваются подъема их на максимально возможную высоту. Характеристики самолетов-разведчиков США приведены в табл. 14.3 [2].

*Таблица 14.3*

| *Тип* | *Скорость, км/ч* | *Дальность полета, км* | *Потолок, м* | *Аппаратура* |
|---|---|---|---|---|
| RF-4C, E | 2240 | 4300 | 18500 | АФА, ИК, ТА, РЛС |
| U-2C | 850 | до 7000 | 26000 | АФА, РРТР, ИК, РЛС |
| SR-71 | 3300 | 7000 | 24000 | То же |
| TR-1 | 690 | 5000 | 27500 | То же |

*Примечание.* АФА — авиационная фотоаппаратура, РРТР — средства радио- и радиотехнической разведки, РЛС — радиолокационные станции бокового обзора, ИК — средства наблюдения в ИК-диапазоне, ТА — аппаратура телевизионного наблюдения.

Дальность наблюдения с самолета наземных объектов зависит от способа добывания и колеблется от 2–3 h для фото- и ИК-аппаратуры, где h — высота полета самолета, до 100–120 h для Р и РТР. При этом достигается разрешение на местности от единиц см (для

фотосъемки) до метров — для радиолокационных станций бокового обзора.

Разрешение и точность определения координат наземных объектов с самолетов выше аналогичных характеристик аппаратуры КА в пропорции, соответствующей соотношению высот полетов.

Возможности добывания информации с кораблей, находящихся в нейтральной зоне возле морских границ, ограничиваются в основном перехватом радиосигналов, наблюдением берегов и их подводного рельефа.

Улучшение характеристик космических и воздушной радиолокационных систем радиоэлектронной разведки происходит за счет использования широкополосных и сверхширокополосных излучаемых сигналов и широкополосных синтезированных апертур. Возможности радиолокационного наблюдения с помощью таких сигналов приблизили разрешение на местности по наклонной дальности и азимуту к предельно достижимым значениям, равным 0,5 и 0,25 длины волны соответственно. Проявляются две тенденции в развитии средств радиолокационного наблюдения:

- использование мм-диапазона с целью повышения разрешающей способности радиолокационных станций;
- смещение рабочего диапазона частот в метровый диапазон для обеспечения более эффективного обнаружения замаскированного объекта.

За счет широкополосных сигналов и больших апертур разрешение на местности перспективных радиолокационных станций, устанавливаемых на беспилотных летательных аппаратах, составит 0,3–0,5 м, а размещаемых на космических аппаратах — до 1 м при зоне обзора более 100 км.

Обобщенные возможности технической разведки по видам носителей ее средств представлены в табл. 14.4.

*Таблица 14.4*

| № п/п | Характеристика средств технической разведки | Возможности видов технической разведки | | | |
|---|---|---|---|---|---|
| | | наземная | космическая | воздушная | морская |
| 1 | Дальность, км | наз. РЭС — 100–250, воз. РЭС — до 500, фото — до 5, ПНВ — до 3, ПЭМИН, ЗУ — 1; направленный микрофон. — 50–75 м | 120–40000 | РРТР (h = 20 км): наз. РЭС — 650, воз. РЭС — до 1000, РЛС БО — 150 | наз. РЭС — до 65, воз. РЭС — до 500, с сам. МА: наз. — до 350, воз. — до 900 |
| 2 | Диапазон частот | 300 Гц–40 ГГц | | | |
| 3 | Разрешение на местности | | фото (h = 120–130 км) — 10–15 см, РЛС БО — 1 м | фото — 5 см, РЛС БО — 0,5 м | |
| 4 | Полоса обзора | | | фото — 5–6 h, ИК — 2–3 h, РЛС БО — 10–12 h, РРТР — 100–120 h | |

*Примечание.* h — высота полета летательного аппарата, МА — морская авиация, РЛС БО — радиолокационная станция бокового обзора, ИК — средство инфракрасной разведки, РРТР — средство радио- и радиотехнической разведки, МА — морская авиация.

Как следует из данных этой таблицы, показатели технической разведки в целом обеспечивают возможность добывания информации в очень большом диапазоне дальностей, частот сигналов и разрешающей способности средств наблюдения.

## Вопросы для самопроверки

1. Основные органы системы разведки.
2. Классификация технических средств добывания информации по назначению.
3. Классификация средств добывания по условиям эксплуатации.
4. Почему мобильные средства имеют худшие характеристики, чем стационарные?
5. Показатели технических средств, существенно влияющие на эффективность добывания информации.
6. Виды орбит разведывательных космических аппаратов.
7. Преимущества и недостатки средств разведки на КА.
8. Разрешающая способность на местности средств наблюдения.

# Глава 15. Технические средства подслушивания

## 15.1. Акустические приемники

Непосредственное (ушами) подслушивание ограничено малым расстоянием от источника звука — в лучшем случае около десяти метров. Малая дальность непосредственного подслушивания обусловлена не только малой мощностью акустических сигналов и большим затуханием их в среде распространения, но и тем, что уши человека имеют широкую диаграмму направленности (близкую к 180°), в силу чего на барабанную перепонку поступают практически все внешние акустические шумы.

Кроме того, шумы поднимают порог чувствительности слуховой системы человека. Но одновременно это физиологическое свойство слуховой системы человека позволяет ему адаптироваться к зашумленности среды обитания, например в жилых помещениях возле транспортных магистралей большого города.

Для непосредственного подслушивания в условиях города злоумышленнику необходимо приблизиться к источнику информации на несколько метров, что существенно ухудшает скрытность добывания информации.

Технические средства подслушивания расширяют и дополняют возможности слуховой системы человека за счет:

- приема и прослушивания акустических сигналов, распространяющихся в воде и твердых телах;
- повышения дальности подслушивания речевой информации по сравнению с непосредственным подслушиванием;
- коррекции спектра акустического сигнала, распространяющегося в среде с неравномерной амплитудно-частотной характеристикой коэффициента передачи или затухания;
- выделения акустического сигнала из смеси его и шумов;
- прослушивания речи, выделяемой из перехваченных радио- и электрических сигналов функциональных каналов связи и из сигналов побочных излучений и наводок;
- ретрансляции добываемой речевой информации на сколь угодно большое расстояние.

Конкретный способ подслушивания реализуется с использованием соответствующих технических средств. Совокупность технических средств, обеспечивающих функции добывания семантической и признаковой акустической информации, представляет собой комплекс средств подслушивания. Структурная схема типового комплекса приведена на рис. 15.1.

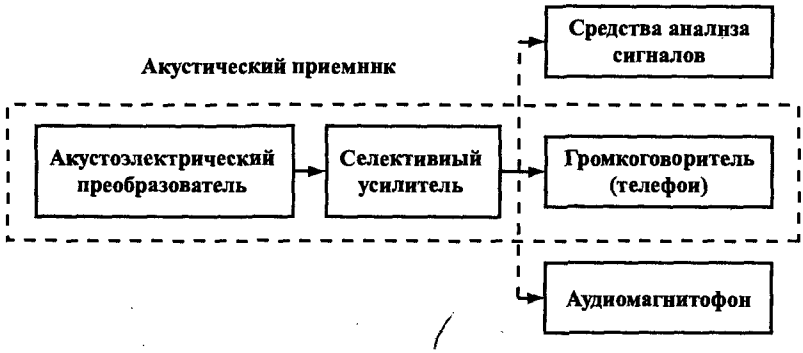



*Рис. 15.1.* Структурная схема комплекса средств подслушивания

Основной частью комплекса является **акустический приемник**. Он производит селекцию по пространству и частоте акустических сигналов, распространяющихся в атмосфере, воде, твердых телах, преобразует их в электрические сигналы, усиливает и обрабатывает электрические сигналы и преобразует их в акустическую волну для обеспечения восприятия информации слуховой системой человека. Акустический приемник содержит акустоэлектрический преобразователь, селективный усилитель и электроакустический преобразователь (телефон, громкоговоритель).

Акустические приемники для приема акустической волны, распространяющейся в воздухе, воде, твердой среде (в инженерных конструкциях), в грунте, отличаются видом акустоэлектрического преобразователя. Иногда по виду акустоэлектрического преобразователя называют весь акустический приемник. Акустоэлектрический преобразователь акустической волны, распространяющейся в воздухе, называется **микрофоном**, преобразователь волны, распространяющейся в твердой среде, — **стетоскопом** и **акселерометром**, в земной поверхности — **геофоном**, а в воде — **гидрофоном**. Основную долю функциональных акус-

тоэлектрических преобразователей акустических приемников составляют микрофоны.

Так как электрические сигналы на выходе акустоэлектрических преобразователей крайне малы и могут принимать значения единиц мкВ, то для их усиления до необходимых для последующего применения величин (единиц В) используется **селективный усилитель**. Его селективность обеспечивается регулируемой полосой пропускания, необходимой для устранения помех на частотах вне спектра акустического сигнала. Учитывая, что затухание среды распространения акустического сигнала увеличивается с повышением его частоты, коэффициент усиления селективного усилителя соответственно повышают для более высоких спектральных составляющих принимаемого сигнала. Такая компенсация эквивалентна повышению уровня акустического сигнала в точке приема до 6 дБ.

Электрический сигнал преобразуют в акустический сигнал, воспринимаемый человеком, **громкоговорители** и **телефоны**. По способу преобразования электрических сигналов громкоговорители разделяются на электродинамические, электромагнитные, электростатические, пьезоэлектрические и др., по виду излучения — на громкоговорители непосредственного излучения, диффузорные и рупорные, по воспроизводимому диапазону частот — на широкополосные, низкочастотные, средне- и высокочастотные. Значения мощности громкоговорителей образуют стандартный ряд в диапазоне 0,1–50 Вт.

Чем уже диапазон частот динамической головки громкоговорителя, тем равномернее ее амплитудно-частотная характеристика, тем меньше головка искажает сигнал. Для высококачественной электроакустической аппаратуры к выходу усилителя подключают несколько динамических головок с разными диапазонами частот, перекрывающими весь звуковой диапазон (16–20000 Гц). Для воспроизводства речи средствами добывания требования к электродинамическим головкам более чем скромные: единицы Вт по мощности и по диапазону частот, соответствующему стандартному телефонному каналу (300–3400 Гц).

Для консервации акустической информации электрический сигнал с выхода акустического приемника подается на **аудиомаг-**

**нитофон**. Для записи акустических сигналов применяют многоканальные стационарные ленточные магнитофоны, портативные лентопротяжные кассетные магнитофоны и специальные носимые лентопротяжные и цифровые диктофоны.

Сигнальные демаскирующие признаки определяются с помощью **средств технического анализа**. Если акустический сигнал на выходе приемника сильно зашумлен, то его электрический аналог подвергают для снижения уровня шума дополнительной обработке. Основу методов очистки электрического сигнала от шума составляют методы **адаптивной фильтрации**. Суть адаптивной фильтрации состоит в том, что на основе анализа поступающего на вход фильтра зашумленного речевого сигнала непрерывно фильтром линейного предсказания «предсказывается» помеховый сигнал, который вычитается затем из смеси речевого сигнала и шума. В результате этого отношение сигнал/шум на выходе фильтра увеличивается.

Возможности акустического приемника характеризуются набором показателей:

- диапазоном частот принимаемого акустического сигнала;
- чувствительностью;
- динамическим диапазоном;
- масса-габаритными характеристиками.

Так как речь является основным видом информации при подслушивании, то большинство акустических приемников для добывания информации работают в речевом диапазоне частот. В отдельных случаях ценной является информация, переносимая акустической волной в инфразвуковом и ультразвуковом диапазонах. К такой информации относятся звуки движущихся объектов (людей, техники, подводных и надводных кораблей и др.), акустические сигналы взрывов новых боеприпасов, разрабатываемых работающих двигателей и других объектов разведки.

Дальность подслушивания (длина простого акустического канала утечки информации) зависит от ряда факторов, в том числе от чувствительности акустического приемника. Под его **чувствительностью** понимается минимальная энергия акустической волны или оказываемое ею минимальное давление, при котором обес-

печивается определенный уровень электрического или акустического сигналов на выходе акустического приемника.

**Динамический диапазон** акустического приемника характеризуется диапазоном в дБ мощности акустического сигнала на его входе (громкости звука), при котором обеспечивается требуемый или допустимый уровень сигнала на выходе акустического приемника. Учитывая, что акустический приемник при добывании информации размещается скрытно, далеко не в оптимальных условиях, его динамический диапазон является важнейшей характеристикой акустического приемника. Например, если динамический диапазон закладного подслушивающего устройства мал, то приемлемое качество добываемой речевой информации обеспечивается лишь в небольшом интервале расстояний от микрофона говорящего человека. Когда разговаривающий человек ходит по комнате, то добываемая информация может содержать участки с плохим качеством речи.

Так как акустические каналы утечки информации имеют малую протяженность и акустический приемник необходимо приблизить к источнику акустического сигнала, то большинство акустических приемников относятся к классу носимой аппаратуры с автономными источниками питания. Поэтому важное значение для практического применения акустического приемника имеют его вес и габариты, а также длительность непрерывной работы.

Для запоминания (записи) добываемой информации сигнал с выхода передается по организуемому каналу связи к запоминающему устройству или записывается в запоминающем устройстве, размещенном в месте нахождения акустического приемника. В последнем варианте к запоминающему устройству предъявляются такие же жесткие требования, как к акустическому приемнику.

Для записи речевой информации широко применяются **специальные диктофоны**, конструктивно объединяющие акустический приемник и запоминающее устройство (лентопротяжный и цифровой магнитофоны). Основными характеристиками запоминающих устройств являются объем памяти в МБайтах, время записи речевой информации в минутах или часах, время непрерывной работы в часах.

**Средства технического анализа** измеряют технические характеристики (сигнальные признаки) акустических сигналов, которые могут использоваться для обнаружения и распознавания их источников: частоту колебаний, характеристики спектра, амплитуду и мощность сигнала и др. Каждый объект с движущимися механическими частями имеет индивидуальную сигнальную признаковую структуру, по которой с достаточно высокой вероятностью можно обнаружить объект и распознать его отдельные свойства. Средства анализа акустических сигналов устанавливаются, например, на подводных лодках для обнаружения и распознавания типов (вплоть до номера) надводных и подводных кораблей.

**Микрофон** как основной и наиболее широко применяемый элемент акустического приемника можно представить в виде последовательного ряда функциональных звеньев. В первом акустическом звене в результате взаимодействия конструкции микрофона и звукового поля формируется механическая сила, зависящая от громкости звука, частоты звукового сигнала, размеров и формы корпуса микрофона и его акустических входов, расстояния между ними и угла падения звуковой волны относительно оси микрофона. Первое звено определяет **характеристику направленности** микрофона и по существу представляет собой акустическую антенну.

Второе звено обеспечивает преобразование механической силы акустической волны в колебания подвижной части микрофона — мембраны. Его свойства определяются расположением, величиной и частотной зависимостью входящих в него акусто-механических элементов. Это звено определяет **амплитудно-частотную характеристику** (АЧХ) микрофона.

Третье звено представляет собой электромеханический преобразователь колебаний мембраны в электрический сигнал и определяет **чувствительность** микрофона. Четвертое электрическое звено выполняет функцию согласования преобразователя с последующей электрической цепью и характеризуется **внутренним** или **выходным сопротивлением** микрофона как источника сигнала.

При подключении микрофона к входным цепям усилителя (нагрузке) с комплексным сопротивлением $Z_н$ напряжение на нем равно $U_н = E_м Z_н / (Z_м + Z_н)$, где $E_м$ и $Z_м$ — выходные напряжения и сопротивление микрофона (рис. 15.2).

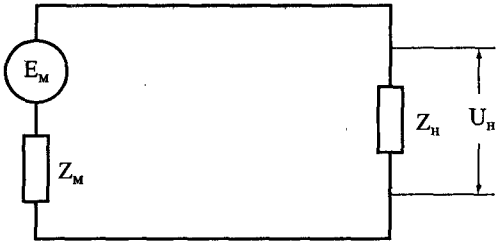



*Рис. 15.2.* Эквивалентная электрическая схема микрофона

Напряжение на нагрузке максимально, т. е. $U_н \to E_м$, при $Z_м << Z_н$. Следовательно, для повышения напряжения на нагрузке необходимо выполнить условие $Z_н >> Z_м$.

Микрофоны классифицируются по различным признакам, указанными на рис. 15.3.

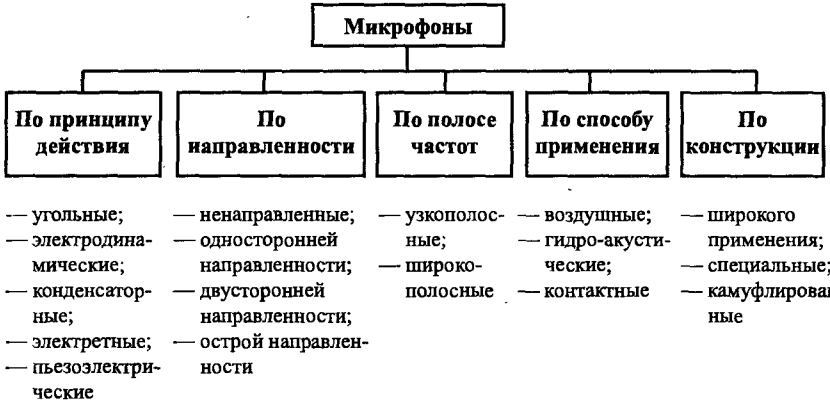



*Рис. 15.3.* Классификация микрофонов

**Угольный (порошковый) микрофон**, впервые созданный в 1879 г. русским инженерном М. Михальским, представляет собой круглую коробочку с гранулированным древесным углем, закрываемую тонкой металлической упругой крышкой — мембраной. К электроду, укрепленному на дне коробочки, и мембране подводится постоянное напряжение, под действием которого в массе угольного порошка протекает электрический ток. Принцип работы угольного микрофона основан на изменении под действием акустической волны сопротивления угольного порошка, находящего-

ся между мембраной и неподвижным электродами. Акустическая волна приводит мембрану микрофона в колебательное движение, вследствие чего изменяется степень сжатия угольного порошка и площадь соприкосновения его гранул друг с другом. В результате этого сопротивление порошка и сила протекающего через него тока меняются в соответствии с громкостью звука, т. е. производится амплитудная модуляция электрического тока. Номинальное сопротивление угольного микрофона зависит от зернистости и технологии обработки порошка и других факторов. Это сопротивление может составлять у низкоомных микрофонов 35–65 Ом, среднеомных — 65–145 Ом и высокоомных — 145–300 Ом. Угольные микрофоны имеют низкую стоимость, высокую чувствительность, обеспечивают возможность без дополнительного усиления передачу электрических сигналов на большие (десятки км) расстояния. Это обстоятельство обуславливает широкое применение угольных микрофонов в проводной телефонной связи. Однако они узкополосные и для передачи более широкополосных, чем речь, акустических сигналов не применяются.

Конструкция **электродинамического микрофона**, изобретенного американскими учеными Э. Венте и А. Терас в 1931 г., аналогична конструкции электродинамического громкоговорителя. В нем катушка из тонкой проволоки жестко связана с мембраной из полистирольной пленки или алюминиевой фольги и постоянно находится в воздушном зазоре постоянного магнита. При колебаниях катушки в ней возникает ЭДС, значение которой пропорционально громкости звука. Динамические микрофоны относительно просты, надежны в работе в широком диапазоне температур и влажности, устойчивы к сотрясениям и широко применяются в различной звукоусилительной и звукозаписывающей аппаратуре.

В **электромагнитном микрофоне** в результате колебаний мембраны из ферромагнитного материала в обмотке неподвижной катушки с сердечником, по которой протекает постоянный ток, возникает ЭДС индукции, величина которой эквивалентна интенсивности звука.

**Конденсаторный микрофон**, изобретенный американским ученым Э. Венте в 1917 г., представляет собой капсюль, состоящий из двух параллельно расположенных пластин — электродов, один

из которых массивный, другой — тонкая мембрана. Электроды образуют конденсатор, емкость которого зависит от площади пластин и расстояния между ними. К электродам подводится через резистор поляризующее постоянное напряжение. При воздействии на мембрану звуковых волн изменяются расстояния между электродами и, соответственно, емкость конденсатора. В результате этого через резистор протекает ток, амплитуда которого пропорциональна звуковому давлению на мембрану. При расстоянии между обкладками 20–40 мкм и поляризующем напряжении в несколько десятков вольт чувствительность микрофона достигает 10–20 мВ/Па.

Разновидностью конденсаторного микрофона является **электретный микрофон**, мембрана которого выполнена из полимерных материалов (смол), способных в сильном электрическом поле и при высокой температуре заряжаться и сохранять электрический заряд продолжительное время. Такие материалы называют **электретами**. Мембрана из электрета металлизируется, между пластинами после заряда возникает разность потенциалов 45–130 В. Электретные микрофоны не нуждаются во внешнем источнике и широко применяются в звукозаписывающей аппаратуре, в том числе для негласного подслушивания.

Действие **пьезоэлектрического микрофона** основано на возникновении ЭДС на поверхности пластинок из пьезоматериала, механически связанных с мембраной. Колебания мембраны под давлением акустической волны передаются пьезоэлектрической пластине, на поверхности которой возникают заряды, величина которых соответствует уровню громкости акустического сигнала.

**По направленности микрофоны** разделяются на **ненаправленные, односторонней, двухсторонней** и **острой направленности**. Направленность микрофона определяется по уровню сигнала на его выходе в зависимости от поворота микрофона по отношению к источнику акустической волны в горизонтальной и вертикальной плоскостях. Ширина диаграммы направленности микрофона оценивается в градусах на уровне 0,5 (0,7) от максимальной мощности (амплитуды) электрического сигнала на его выходе. Чем меньше ширина диаграммы направленности микрофона, тем меньше помех попадает на его мембрану из направлений, отличающихся от направления на источник акустического сигнала

с информацией. Ширина диаграммы направленности микрофонов острой направленности составляет несколько десятков градусов. Пространственное ограничение помех повышает отношение сигнал/помеха на мембране микрофона.

**Частотные искажения** при преобразовании акустической волны в электрический сигнал определяются неравномерностью частотной характеристики микрофона. Она описывается отклонением в процентах или дБ уровня спектральных составляющих звукового сигнала на выходе преобразователя по отношению к уровню спектральных составляющих входного сигнала.

**По диапазону частот** микрофоны разделяются на **узкополосные и широкополосные**. Узкополосные микрофоны предназначены для передачи речи. Широкополосные микрофоны имеют более широкую полосу частот и преобразуют колебания в звуковом и частично ультразвуковом диапазонах частот.

**По способу применения** микрофоны разделяются на **воздушные, гидроакустические (гидрофоны)** и **контактные**. Контактные микрофоны предназначены для приема структурного звука. Например, контактный стетоскопный микрофон UM 012, прикрепленный к стене помещения, позволяет прослушивать разговоры в соседнем помещении при толщине стен до 50 и более см. Модификацией контактных микрофонов являются ларингофоны и остеофоны, воспринимающие и преобразующие в электрические сигналы механические колебания (вибрации) связок и хрящей гортани или кости черепа говорящего. Они встраиваются в шлемы летчиков и танкистов для обеспечения связи в условиях повышенного акустического шума среды.

По **конструктивному исполнению** микрофоны бывают широкого применения, специальные миниатюрные и специальные субминиатюрные, применяемые в различных закладных устройствах.

Возможности микрофонов определяются следующими характеристиками:

- чувствительностью на частоте акустической волны 1000 Гц;
- диаграммой направленности;
- диапазоном воспроизводимых частот колебаний акустической волны;
- неравномерностью частотной характеристики;
- масса-габаритными характеристиками.

**Чувствительность** — один из основных показателей микрофона и оценивается коэффициентом преобразования давления акустической волны в уровень электрического сигнала. Так как чувствительность микрофона для разных частот акустических колебаний различная, то она определяется на частоте 1000 Гц. Измерения проводятся для акустической волны, направление распространения которой перпендикулярно поверхности мембраны, в вольтах или милливольтах на паскаль (В/Па, мВ/Па). Чувствительность микрофона зависит в основном от параметров физических процессов в акустоэлектрических преобразователях и площади мембраны микрофона.

Чувствительность микрофона повышается с увеличением площади мембраны приблизительно в квадратичной зависимости. Например, чувствительность конденсаторного микрофона с диаметром мембраны 6 мм составляет 1,5–4 мВ/Па, для диаметра 12 мм – 12,5 мВ/Па, а при диаметре 25 мм она увеличивается до 50 мВ/Па.

Электрические сигналы на выходе микрофонов, используемых для добывания информации, в селективном усилителе обрабатываются и усиливаются до величины, необходимой для их записи с помощью аудиомагнитофона или преобразования в акустический сигнал для обеспечения восприятия информации человеком.

Обобщенные характеристики акустических микрофонов приведены в табл. 15.1 [3].

*Таблица 15.1*

| *№ п/п* | *Тип микрофона* | *Характеристики:* | | |
|---|---|---|---|---|
| | | *диапазон частот, Гц* | *неравномерность АЧХ, дБ* | *чувствительность на $f$ = 1000 Гц, Вм²/н* |
| *1* | *2* | *3* | *4* | *5* |
| 1 | Угольные порошковые | 200–4000 | 20 | 1000 |
| 2 | Электродинамические | 30–15000 | 12 | 1 |
| 3 | Электромагнитные | 150–5000 | 20 | 5 |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 4 | Конденсаторные (с дополнительным источником напряжения) | 30–15000 | 5 | 5 |
| 5 | Электретные | 20–18000 | 2 | 1 |
| 6 | Пьезоэлектрические | 100–5000 | 15 | 50 |

*Примечание.* Чувствительность микрофона приведена в вольтах при площади мембраны 1 м$^2$ и осевом давлении в 1 Ньютон (Н). В системе СИ эта характеристика измеряется в мВ/Па.

Как следует из этой таблицы, наиболее высокой чувствительностью обладают угольные микрофоны, что обеспечивает им столь длительное использование для передачи речевой информации по телефонным каналам связи. Однако остальные их характеристики (частотный диапазон и его неравномерность) невысокие. По совокупности показателей высокие характеристики имеют электродинамические и конденсаторные микрофоны. Электродинамические микрофоны широко используются для звукоусиления речи и музыки. Конденсаторные микрофоны в силу минимальной неравномерности их амплитудно-частотной характеристики применяют в метрологии для измерения акустических сигналов, а малые размеры электретных микрофонов способствуют их широкому применению в электронной носимой технике.

Увеличение дальности подслушивания акустической информации без повышения мощности ее источника, например громкости речи человека, достигается за счет повышения отношения сигнал/шум на входе акустического приемника. При этом под шумами имеются в виду не только акустические шумы других источников акустических сигналов, но и собственные тепловые шумы входных каскадов акустического приемника. Слуховая система молодого человека как акустический приемник может принимать акустическую информацию очень малой мощности, но вследствие очень широкой диаграммы направленности ушей (почти 180°) на барабанную перепонку приходят шумы со всех направлений. С возрастом чувствительность слуховой системы человека ухудшается.

Млекопитающие, для которых звуки несут важную для жизни информацию, имеют уши с более узкой диаграммой направленности и способностью изменять ее ориентацию в пространстве.

Микрофоны для дистанционного подслушивания имеют акустическую антенну, сужающую его диаграмму направленности. Эти микрофоны называются **остронаправленными микрофонами**. Характер увеличения относительной дальности $R_м/R_0$ остронаправленного микрофона от его коэффициента направленного действия $G_м$ иллюстрируется зависимостью на рис. 15.4 [11].

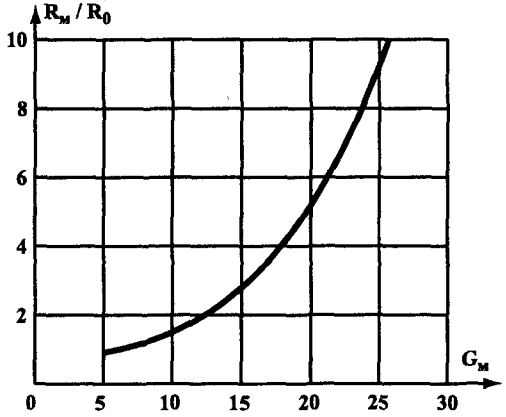



*Рис. 15.4.* Зависимость относительной дальности микрофона от коэффициента его направленного действия

Величины $R_м$ и $R_0$ на рисунке обозначают дальность подслушивания микрофоном и ушами человека соответственно. В качестве микрофона рассматривается гипотетический микрофон с чувствительностью, равной пороговой чувствительности слуховой системы человека.

Различают следующие типы остронаправленных микрофонов:

- параболические;
- трубчатые;
- плоские;
- градиентные.

**Параболический остронаправленный микрофон** содержит отражатель звука параболической формы из оптически прозрач-

ного или непрозрачного материала диаметром 20–50 см, в фокусе которого размещается мембрана микрофона. Звуковые волны с осевого направления отражателя суммируются в фокусе параболического отражателя — на мембране микрофона. Акустические сигналы, распространявшиеся с иных направлений, фокусируются вне мембраны, тем дальше от нее, чем больше угол их прихода по отношению к оси отражателя. Коэффициент направленного действия параболического микрофона можно оценить по формуле: $G_п = 4\pi^3 d^2 / \lambda^2$, где d — диаметр отражателя, $\lambda$ — длина волны звука. Например, для d = 30 см и звука на f = 1000 Гц ($\lambda$ = 34 см) $G_п \approx 24$ дБ. Для сравнения, среднее значение $G_0$ ушей человека оценивается величиной всего в 6 дБ.

**Трубчатый (интерференционный, «бегущей волны») остронаправленный микрофон** состоит из одной трубки длиной 0,2–1 м и толщиной 10–30 мм или набора трубок, длины которых пропорциональны длинам волн спектральных составляющих акустического сигнала. В торце трубок укрепляется мембрана микрофона. Принцип действия однотрубчатого микрофона иллюстрируется на рис. 15.5.

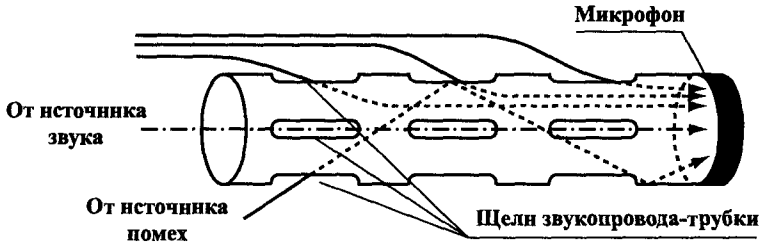



*Рис. 15.5.* Принцип действия трубчатого микрофона

Трубка-звуковод имеет щелевые отверстия, размещенные рядами по длине трубки. Когда ось трубки направлена на источник звука, то акустические волны от него, проникающие в трубку через ее открытый торец и щели, складываются на мембране микрофона в фазе, так как проходят приблизительно одинаковый путь. Фазы акустических волн с иных направлений имеют на мембране микрофона различные фазы, вплоть до противоположной. В результате этого диаграмма направленности трубчатого микрофона сужается. Коэффициент направленного действия такого микрофона длиной

L при условии, что $L > \lambda$, оценивается формулой $G_т \approx 4L / \lambda$. Для $L = 1$ м и $f = 1000$ Гц $G_т \approx 12$ дБ.

**Плоский микрофон** представляет собой фазированную акустическую решетку, в узлах которой размещаются микрофоны и сигналы которых суммируются на входе усилителя. Конструктивно он представляет плоскую поверхность с вмонтированными в нее микрофонными капсулями, образующими обычно матрицу $3 \times 3$. Когда поверхность решетки перпендикулярна направлению на источник звука, то фазы электрических сигналов совпадают и суммарный сигнал максимален. При отклонении угла прихода акустических волн от нормального к поверхности мембран микрофонов между сигналами от разных микрофонов возникает разность фаз из-за различий длин путей от источника к разным микрофонам. Уровень суммарного сигнала снижается, что приводит к уменьшению ширины диаграммы направленности микрофона. Коэффициент направленного действия такого микрофона определяется по формуле: $G_{пл} = 4\pi S / \lambda^2$, где S — площадь поверхности, занимаемой микрофонами. Поверхность плоского направленного микрофона встраивается в стенку атташе-кейса или в жилет, носимый под рубашкой и пиджаком. Например, направленный микрофон с акустической решеткой, размещенный на внутренней поверхности верхней крышки кейса, имеет ширину диаграммы направленности около 35°. Принятая речевая информация может быть записана на диктофон в кейсе или ретранслироваться с помощью передатчика на достаточно большое расстояние.

В **градиентных микрофонах** в отличие от плоского микрофона, в котором производится сложение акустических сигналов с элементов приемной фазированной решетки, сигналы соседних элементов вычитаются. В результате этого диаграмма направленности имеет вид cos Q, где Q — угол прихода акустической волны относительно оси микрофона. Коэффициент направленного действия и чувствительность такого микрофона невелики, но в простейшем варианте (2 микрофона) имеют малые размеры.

Рекламируемые возможности по дальности подслушивания направленных микрофонов (до 500 и более метров) завышаются. Из кривой на рис. 15.4 следует, что реальная дальность подслушивания речевой информации на улице города при коэффициенте

направленного действия микрофона 15–20 дБ составляет 10–20 м при дальности непосредственного подслушивания всего 2–4 м. Реальная дальность подслушивания зависит не только от громкости источника звука, его коэффициента направленного действия, но и уровня акустических помех. С учетом имеющихся противоречивых данных предполагается, что максимальная дальность подслушивания разговора с помощью остронаправленных микрофонов может достигать 50–100 м.

Для снятия информации с акустической волны, распространяющейся в твердой среде, применяется **акселерометр**. Он преобразует структурный звук в электрический сигнал, величина которого пропорциональна амплитуде смещения частиц твердого вещества, скорости или ускорения его частиц при распространении структурного звука. В широко распространенных пьезоэлектрических акселерометрах одна или две пластины из пьезоэлемента размещаются между основанием, прикрепляемым к вибрирующей поверхности, и массивной накладкой (рис. 15.6).

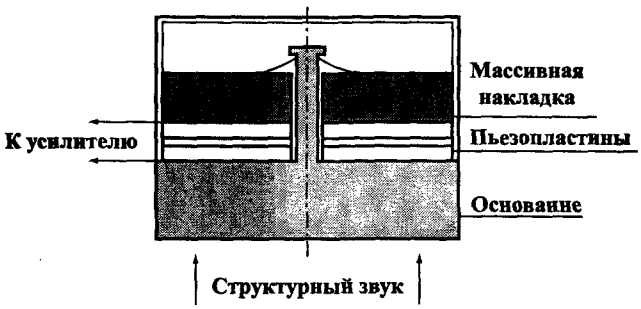



*Рис. 15.6.* Конструкция акселерометра

Колебания твердой среды через основание акселероментра передаются на контактирующую с ним нижнюю поверхность пьезоэлемента. Другая (верхняя) поверхность пьезоэлемента прилегает к массивной прокладке, которая из-за ее инерционности практически остается неподвижной. В силу этого пьезоэлемент подвергается давлению, пропорциональному разности ускорений сил, действующих на обе его поверхности. В результате этого на обкладках пьезоэлемента возникают электрические сигналы, соответствующие структурному звуку.

Для преобразования структурного звука в воздушную акустическую волну, передаваемую по звукопроводам в уши человека, применяется технический **стетоскоп**. Он отличается от медицинского, применяемого для прослушивания акустических сигналов в теле человека, конструкцией мембраны, поверхность которой согласуется с поверхностью вибрирующей твердой среды. Стетоскоп представляет собой один или два гибких звукопровода в виде резиновых или из других синтетических материалов трубок, соединенных с контактной площадкой и передающих звуковое колебание от поверхности твердого тела к ушам человека. Эти звукопроводы локализуют и направляют звуковую волну к ушам человека, а также изолируют ее от акустических помех в окружающем пространстве. Для прослушивания структурных звуков микрофон стетоскопа прижимают или приклеивают к поверхности стены или трубы.

Принципы работы гидрофона и геофона близки принципам работы микрофона и акселерометра соответственно, но с иными конструктивными решениями. Например, мембрана гидрофона может иметь цилиндрическую или сферическую форму. Геофоны применяются не только для обнаружения акустических сигналов от движущихся людей или техники, но и для снятия речевой информации с сейсмической волны в грунте на удалении до 10 м от ее источника.

Наряду с традиционными техническими средствами подслушивания с небольшой дальностью все шире применяются устройства, образующие составные каналы утечки: акусто-радиоэлектронные и акусто-оптические. Такими устройствами являются закладные и лазерные средства подслушивания.

## 15.2. Диктофоны

Для скрытого подслушивания речевой информации и ее регистрации широко применяются диктофоны с встроенными и выносными микрофонами. Скрытая запись информации производится с целью:

- «документирования» беседы или телефонного разговора для экономии времени при составлении отчета или для последующего анализа разговора;

- регистрации трудно запоминаемой во время разговора информации;
- использования записи для оказания влияния на собеседника или предоставления ее в качестве доказательства каких-либо его обещаний и высказываний, сбора материалов о конкурентах, злоумышленниках и др.;
- получения голосового образца собеседника для последующей идентификации при подслушивании;
- регистрации собственных предложений для их последующего анализа;
- записи разговора в помещении во время отсутствия владельца диктофона.

Диктофоны по принципам работы делятся на **кинематические** (с лентопротяжным механизмом для обеспечения записи на магнитную ленту или металлическую проволоку) и **цифровые**.

**Кинематические диктофоны** для скрытного подслушивания отличаются от бытовых или профессиональных (используемых журналистами) демаскирующими признаками с пониженной информативностью и возможностью скрытного управления режимами работы. Это достигается:

- уменьшением в результате прецизионного изготовления механических узлов акустических шумов лентопротяжного механизма;
- минимизацией побочных электромагнитных излучений за счет исключения из электрической схемы генераторов подмагничивания и стирания;
- экранированием электромагнитного излучения коллекторного двигателя;
- возможностью подключения выносного микрофона;
- возможностью размещения диктофона и его компонентов в одежде человека и скрытного управления режимами работы диктофона;
- высокой автоматизацией работы диктофона — установкой акустоавтомата, счетчика ленты, автореверса, индикатора работы и другими элементами.

Запись речи в диктофонах производится на микрокассете со скоростью 2,4 или 1,2 см/с, длительность записи в зависимости от скорости и типа кассеты составляет от 15 мин до 3 часов.

Автономное электропитание большинства диктофонов обеспечивается 1–2 элементами химического источника тока типа АА и ААА, вес их с батарейками составляет десятки и сотни г (Olimpus L400, например 90 г), а габариты диктофонов позволяют их размещать во внутреннем кармане пиджака.

Металлические корпуса диктофона и дополнительного кожуха-экрана существенно ослабляют электромагнитное излучение коллекторного двигателя, но не исключают его обнаружение на небольшом удалении в десятки см.

В цифровых диктофонах лентопротяжный механизм отсутствует, а запись речевой информации производится в цифровой форме на полупроводниковых запоминающих устройствах. Отсутствие в цифровых диктофонах лентопротяжного механизма исключает акустические шумы, но в качестве его демаскирующего признака проявляются высокочастотные излучения, создаваемые импульсами тактовой частоты аналого-цифрового преобразователя и полупроводниковой памяти.

## 15.3. Закладные устройства

С целью существенного повышения дальности подслушивания широко применяются закладные устройства (закладки, радиомикрофоны, «жучки», «клопы»). Эти устройства перед подслушиванием скрытно размещаются в помещении злоумышленниками или привлеченными к этому сотрудниками организации, проникающими под различными предлогами в помещение. Такими предлогами могут быть посещения руководства или специалистов посторонними лицами с различными предложениями, участие в совещаниях, уборка, ремонт помещения и технических средств и т. д.

Закладные устройства в силу большого разнообразия конструкций и оперативного применения создают серьезные угрозы безопасности речевой и иной защищаемой информации в местах с ограниченным доступом.

В общем случае закладное устройство представляет собой ретранслятор, на вход которого поступает первичный сигнал, несущий информацию, а на выходе — сигнал, согласованный с характеристиками среды, в котором он будет распространяться. Разнообразие закладных устройств порождает многообразие вариантов их классификаций. Вариант классификации указан на рис. 15.7.


*Рис. 15.7.* Классификации закладных устройств

По виду носителя информации, распространяющейся от закладных устройств, их можно разделить на **проводные** и **излучающие закладные устройства**. Носителем информации от проводных закладок является электрический ток, который распространяется по электрическим проводам, а излучающие закладные устройства передают информацию с помощью радио- и ИК-сигналов.

В зависимости от вида первичного сигнала проводные и излучающие закладные устройства делят на **акустические** и **аппаратные**. Акустические закладные устройства содержат микрофон, преобразующий акустические сигналы в электрические. Аппаратные закладки устанавливаются в телефонных аппаратах, ПЭВМ и других радиоэлектронных средствах. Входными сигналами для них являются электрические сигналы, несущие речевую информацию (в телефонных аппаратах), или информационные последовательности, циркулирующие в ПЭВМ при обработке конфиденциальной информации. В таких закладках отсутствует микрофон, что упрощает их конструкцию, и имеется возможность использовать для электропитания энергию средства, в котором установлена закладка. Информацию аппаратные закладки могут передавать по проводам — проводные аппаратные или с помощью радиосигналов —

излучающие аппаратные. Широко применяются проводные телефонные закладные устройства, ретранслирующие по радиосигналу речевую информацию в телефонных линиях.

Проводные акустические закладки представляют собой:

- субминиатюрные микрофоны, скрытно установленные в бытовых радио- и электроприборах, в предметах мебели и интерьера и соединенные тонким проводом с микрофонным усилителем или диктофоном, размещаемыми в других помещениях;
  миниатюрные устройства, содержащие микрофон, усилитель и формирователь сигнала, передаваемого, как правило, по телефонным линиям и цепям электропитания.

Проводные акустические закладки имеют высокую чувствительность и помехоустойчивость, но наличие дополнительного провода демаскирует закладки и усложняет их установку, в особенности в условиях дефицита времени. Поэтому такие закладки могут устанавливаться во время ремонта или в помещениях с возможностью достаточно простого и длительного доступа в них людей, например в номера гостиниц.

Закладки, использующие санкционированно проложенные провода (цепи электропитания и информационные линии), лишены этого недостатка. Поэтому они все шире применяются для передачи в пределах здания информации в места нахождения злоумышленника или его средства для записи или ретрансляции сигнала по радиоканалу. Эти закладные устройства устанавливаются в местах подключения проводов электропитания к выключателям и сетевым розеткам, в телефонных аппаратах или их розетках, а также внутри иных радиосредств.

Излучающие закладные устройства лишены недостатков проводных, но у них проявляется другой информативный демаскирующий признак — излучения в радио- и оптическом диапазонах.

Наиболее широко применяются акустические радиозакладки, позволяющие сравнительно просто и скрытно устанавливать их в различных местах помещения. Простейшая акустическая радиозакладка содержит (см. рис. 15.8) следующие основные устройства: микрофон, микрофонный усилитель, генератор несущей частоты, модулятор, усилитель мощности, антенну и источник электропитания.

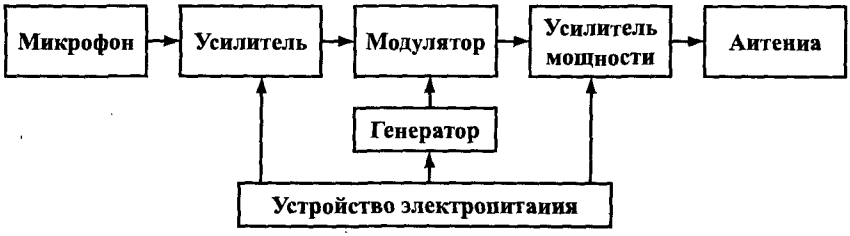



*Рис. 15.8.* Схема акустической закладки

Микрофон преобразует акустический сигнал с информацией в электрический, который усиливается до уровня входа модулятора. В модуляторе производится модуляция колебания несущей частоты усиленным сигналом с микрофона, т. е. информация переписывается с низкочастотного носителя на высокочастотный носитель. Для обеспечения необходимой мощности излучения модулированный сигнал усиливается в усилителе мощности. Электрическая схема современных закладных устройств все чаще дополняется устройствами, обеспечивающими тактическое закрытие передаваемой информации.

Излучение радиосигнала в виде электромагнитной волны осуществляется антенной, как правило, в виде отрезка провода. Для телефонных излучающих закладных устройств в качестве антенны используются провода телефонных линий. Так как антенны в виде кусков провода (диполей) или проводов линий плохо согласуются длинами волн генерируемых передатчиком колебаний, то лишь небольшая часть мощности электрических сигналов излучается в эфир.

В целях сокращения веса, габаритов и энергопотребления в радиозакладке указанные функции технически реализуются минимально возможным количеством активных и пассивных элементов. Простейшие закладки содержат всего один транзистор.

Установка закладных устройств возможна **с заходом** злоумышленника в помещение, где производится их размещение, или **без захода**. Первый вариант позволяет более рационально разместить закладку как с точки зрения энергетики, так и скрытности, но связан с повышенным риском для злоумышленника. Поэтому в случаях, когда создаются предпосылки для дистанционной (беззаходовой) установки закладки, их забрасывают в помещение или ими выстре-

ливают из пневматического ружья или лука. Например, комплект PS фирмы Sipe Electronic состоит из специального бесшумного пневматического пистолета с прицельным расстоянием 25 м и радиозакладкой, укрепленной на стреле. Стрела после выстрела надежно прикрепляется с помощью присоски к поверхностям из металла, дерева, пластмассы, бетона и других гладких строительных и облицовочных материалов. Микрофон обеспечивает съем речевой информации с расстояния до 10 м, а передатчик — ее передачу на расстояние до 100 м.

По **диапазону частот** закладные устройства отличаются большим разнообразием. На ранних этапах использования закладных устройств частоты излучений их привязывали к частотам бытовых радиоприемников в УКВ-диапазоне. При массовом появлении у населения бытовых радиоприемников увеличилась опасность случайного перехвата сигналов радиозакладок посторонними лицами. Поэтому большинство типов современных закладок имеют более высокие частоты в УВЧ-диапазоне.

Для более 96% радиозакладок рабочие частоты сосредоточены в интервале 88–501 МГц, причем большая часть (52%) из них имеет частоты 373–475 МГц, около 42% — 92–169 МГц [4]. Наиболее интенсивно используется диапазон частот 450–475 МГц, в котором сосредоточены рабочие частоты 36% имеющихся на рынке радиозакладных устройств.

Продолжается тенденция дальнейшего повышения частот, в том числе с переходом в ГГц-диапазон. С увеличением частоты передатчика уменьшается уровень помех, что позволяет снизить мощность передатчика и, соответственно, его габариты, а также длину антенны. Кроме того, железобетонные стены помещений современных зданий экранируют излучаемое закладным электромагнитное поле тем больше, чем больше длина волны по отношению к линейным размерам ячейки железной арматуры стены. Поэтому с повышением частоты передатчика закладного устройства (уменьшением длины волны) экранирующий эффект арматуры железобетонной стены понижается, хотя затухание поля в бетоне несколько увеличивается.

В интересах повышения скрытности для излучающих закладных устройств осваивается ИК-диапазон. Однако в силу большего по сравнению с радиоволнами затухания ИК-лучей в среде распро-

странения и необходимостью обеспечения прямой видимости между излучателем ИК-закладки и фотоприемником злоумышленника применение подобных закладных устройств ограничено.

Кроме диапазона частот на условия передачи закладкой информации влияет стабильность частоты ее передатчика. Для простых схемных решений передатчика закладки значения его частоты изменяются в значительных пределах в зависимости от температуры и питающего напряжения. Величина дрейфа рабочей частоты радиозакладок может достигать единиц МГц. В результате этого радиоприемник, настроенный на частоту радиозакладки, через некоторое время «теряет» радиосигнал. Это обстоятельство имеет важное значение для обеспечения автоматического приема сигналов радиозакладок, например, в случае, когда подслушивание производится аппаратурой в автомобиле при отсутствии в нем оператора. Частоты около половины предлагаемых на рынке радиозакладок стабилизируются.

Повышение стабильности частоты излучения обеспечивается путем применения в колебательном контуре генератора элементов со слабой температурной зависимостью, температурной компенсации, стабилизации питающих напряжений, включения в колебательный контур элементов, стабилизирующих его частоту.

Различают «мягкую» и «жесткую» стабилизацию. В закладных устройствах «мягкая» стабилизация со стабильностью частоты $10^{-3}$–$10^{-4}$ достигается схемотехническими решениями (стабилизацией напряжения, температурной компенсацией и др.). Для большей стабильности частоты передатчика («жесткой», со стабильностью $10^{-5}$–$10^{-6}$) в качестве стабилизирующих элементов используются пластины кристалла кварца. При установке кварца параллельно контуру генератора в нем возникают стабильные механические колебания, частота которых зависит от вида среза кристалла кварца, толщины и размеров его пластины. Резонансные электрические колебания в контуре существуют при равенстве частот колебаний кварца и контура. Стабилизация частоты излучения радиозакладки усложняет ее схему и увеличивает габариты передатчика, но существенно улучшает удобство работы.

Другой проблемой, возникающей при применении закладных устройств, является обеспечение их энергией в течение времени подслушивания. Возможности современной микроэлектроники по

созданию миниатюрных закладных устройств ограничиваются, в основном, масса-габаритными характеристиками автономных источников питания (химических элементов). Микрогабаритные источники тока, широко применяемые в электронных часах, обеспечивают работу закладных устройств в течение короткого времени (десятков часов при минимально-допустимой мощности излучений для дальности до сотни метров). Для закладных устройств используются гальванические элементы (батареи и аккумуляторы) с высокой удельной емкостью. Усредненные характеристики таких элементов приведены в табл. 15.2.

*Таблица 15.2*

| *Тип элемента* | *Напряжение, В* | *Удельная емкость, Втч/кг* | *Саморазряд, % в месяц* |
|---|---|---|---|
| Никель-кадмиевый (Ni-Cad) | 1,25 | 40–80 | 20 |
| Никель-гидридный (Ni-MH) | 1,25 | 60–120 | 30 |
| Литий-ионный (Li-Ion) | 3,6 | 110–160 | до 10 |
| Литий-полимерный (Li-Pol) | 3,6 | 100–130 | до 10 |

Емкость гальванического элемента пропорциональна его габаритам и весу. Наиболее широко распространены цилиндрические гальванические элементы размером АА и ААА с диаметром 10,5 и 8,2 мм, высотой 44,5 и 40,2 мм соответственно. Кнопочные (в виде таблетки) гальванические элементы имеют диаметр 7,86–16 мм и высоту 3,56–16,8 мм. Плоские элементы имеют габариты: длина 14,2–31 мм, высота 14–21,4 мм. В крупногабаритных закладных устройствах применяют ядерные источники электропитания с временем работы в десятки лет, но нуждающиеся в толстых и тяжелых экранах для защиты от радиоактивного излучения.

Радикально проблема электропитания закладных устройств и, соответственно, продолжительности их работы решается подключением закладных устройств к внешним источникам электропитания — к сети и цепям РЭС и других приборов, в которые устанавливаются закладные устройства. Широко применяются подобные закладные устройства в телефонных аппаратах, закамуфлированные под их элементы (конденсаторы, телефонные капсюли и др.), в тройниках для подключения нескольких приборов к одной розет-

ке электросети. По оценке, приведенной в [4], в 75% закладных устройств используется автономное (батарейное) питание, 8% — питание от сети и 17% — питание от телефонной линии. Кроме того, энергия может подводиться извне путем облучения закладных устройств внешним электромагнитным полем. Возможность их непрерывной работы до момента обнаружения и изъятия объясняет все более широкое их распространение.

Увеличение времени эксплуатации и повышение скрытности работы закладного устройства достигаются также путем автоматического подключения к автономному источнику питания наиболее энергоемкого узла радиозакладки — передатчика только в период передачи речевой информации. Такая возможность реализуется в двух вариантах. В первом варианте в закладке устанавливается специальное устройство — акустический автомат (акустоавтомат), подключающее к источнику питания передатчик при приеме закладкой акустического сигнала.

В тишине, в ночное время во включенном состоянии (в «дежурном» режиме) находится лишь микрофонный усилитель с исполнительным электронным реле. При появлении в помещении акустических сигналов от разговаривающих людей реле по сигналу от микрофонного усилителя подключает передатчик и закладное устройство излучает радиосигналы с информацией. После прекращения разговора исходное состояние реле восстанавливается и излучение прекращается.

Во втором варианте дистанционно управляемые закладные устройства включаются на излучение по внешнему радиосигналу, подаваемому злоумышленником. Эти закладные устройства обеспечивают повышенную скрытность и более длительное время работы. Однако для их эффективного применения надо иметь дополнительный канал утечки сведений о времени циркулирования конфиденциальной информации в помещении, где установлено закладное устройство. Например, надо достаточно точно знать время, когда будут вестись в помещении конфиденциальные разговоры. Так как дистанционно управляемые закладки содержат устройство для приема управляющих радиосигналов, то они наиболее сложные и, следовательно, дорогие.

С целью дополнительного повышения скрытности работы закладных устройств все шире применяют преобразования сигналов, затрудняющих их обнаружение. По этому признаку закладные устройства делят на незакрытые и с техническим закрытием.

Жесткие требования к габаритам, массе, энергопотреблению закладных устройств ограничивают мощность излучения их передатчиков. Наиболее часто (более 80%) применяются радиомикрофоны, мощность излучения которых находится в интервале 3–11 мВт, закладки с более высокой мощностью — до 22 мВт составляют менее 10% . Встречаются закладки и большей мощности излучения (до 200 мВт и более), однако их доля крайне незначительна. Малая мощность излучения передатчиков радиозакладок определяет относительно небольшую дальность приема их сигналов. Около 75% образцов обеспечивает функционирование канала на расстояниях 50–350 м, 16% — на расстояниях 460–600 м, 7% — на расстояниях 740–800 м и только около 2% — на расстоянии до 1000 и более метров. Указанные пропорции со временем меняются, но их характер сохраняется.

В общем случае технические данные закладных устройств находятся в следующих пределах:

- частотный диапазон — 27–900 МГц;
- мощность — 0,2–500 мВт;
- дальность — 10–1500 м;
- время непрерывной работы — от нескольких часов до нескольких лет;
- габариты — 1–8 дм$^3$;
- вес — 5–350 г.

Основная проблема оперативного применения закладных устройств заключается в рациональном размещении их в помещении или в радиоэлектронном средстве. Рациональность достигается при обеспечении:

- поступления на вход закладки сигнала с характеристиками, необходимыми для качественной передачи звуковой или иной информации;

- скрытности размещения и работы закладки, по крайней мере, в течение времени подслушивания интересующей злоумышленника информации.

Эффективность выполнения этих условий зависит от удаленности места установки закладки от источников звука и наличия между ними звукопоглощающих и звукоизолирующих экранов, от чувствительности микрофона, размеров и параметров акустики, прежде всего, от времени реверберации помещения и времени, которым располагает злоумышленник для установки. Чувствительность современных малогабаритных микрофонов обеспечивает достаточно качественный прием акустических сигналов на удалении до 10–15 м при отсутствии экранов на пути распространения акустической волны. На качество речи, ретранслируемой закладным устройством, влияют:

— соотношение сигнал/шум на входе микрофонного усилителя закладного устройства;
— время реверберации помещения, в котором установлено закладное устройство.

При малом времени реверберации на микрофон закладки поступает прямая акустическая волна, ослабленная расстоянием и экранами, маскирующими закладку. При большом времени уровень сигнала на мембране увеличивается за счет энергии переотраженных волн, но вследствие сложения на мембране волн, соответствующих разным звукам, ухудшается разборчивость ретранслируемой речи. Эти факторы влияют на качество восприятия такой речи человеком, но в меньшей степени, чем при ретрансляции ее закладными устройствами.

Несмотря на сравнительно малые размеры и вес закладных устройств, они могут быть обнаружены при тщательном визуальном осмотре помещения. С целью продления времени их оперативного использования, а также приближения микрофонов к источнику звука закладные устройства камуфлируют под предметы, не вызывающие подозрение у окружающих людей. Трудно назвать предметы личного пользования, средства оргтехники, средства бытовой радиоэлектроники, в которые не устанавливались бы различные устройства для подслушивания. Некоторые из таких средств подслушивания приведены в табл. 15.3.

*Таблица 15.3*

| *Наименование средства* | *Тип, фирма* | *Характеристики средства* |
|---|---|---|
| Радиопередатчики в: | ELECTRONIC: | |
| стакане | PK535 | 65 × 100 мм, 210 г, солнечные батареи |
| пепельнице | PK565-S | 90 × 45 мм, 480 г, солнечные батареи |
| подсвечнике | PK580 | 100 × 175 мм, 650 г, солнечные батареи |
| калькуляторе | PK620-S | 135 × 100 мм, радиус действия 150–200 м |
| розетке электропитания | PK550 | 140 × 60 × 40 мм, 380 г, дальность до 600 м |
| настольной зажигалке | PK575 | 80 × 32 × 52 мм, 150 г, время работы до 80 ч |
| гвозде | PK520 | 35 × 6 мм, 96 г, 36 часов, до 200 м |
| шариковой ручке | PK585 | 135 × 11 мм, 25 г, 6 часов, до 300 м |
| часах | PK1025-S | 88–108 или 130–150 МГц, 6 часов |
| ремне | PK850-S | 139 МГц, до 800 м |
| Радиопередатчик в запонках, булавке для галстука | STG 4140, STG | 15–150 МГц, мощность 5 мВт |
| Радиопередатчик в видеокассете | UM 007.3, SMIRAB ELECTRONIC | 136–146 МГц, до 300 м, время непрерывной работы 3 суток |
| Магнитофон в книге | PK660, ELECTRONIC | 200 × 250 × 65 мм, 1200 г, время записи 2 × 90 мин. |
| Магнитофон в пачке сигарет | PK1985, ELECTRONIC | 55 × 87 × 21 мм, 160 г, время работы 11 час. |

## 15.4. Лазерные средства подслушивания

Подслушивание с помощью лазерных средств является сравнительно новым способом (первые рабочие образцы появились в 60-е годы) и предназначено для съема акустической информации с плоских вибрирующих под действием акустических волн поверхностей. К таким поверхностям относятся, прежде всего, стекла закрытых окон.

Система лазерного подслушивания состоит из лазерного передатчика в инфракрасном диапазоне и оптического приемника. Лазерный луч с помощью оптического прицела направляется на окно помещения, в котором ведутся интересующие злоумышленника разговоры. При отражении лазерного луча от вибрирующей поверхности происходит его частотная, угловая и фазовая модуляция.

Частотная модуляция обусловлена эффектом Допплера вследствие колебательных движений оконного стекла под воздействием акустического речевого сигнала. Но этот вид модуляции из-за проблемы измерения изменений частоты (длины волны) для добывания информации не используется.

Изменение угла отражения лазерного луча, т. е. угловая модуляция, происходит из-за искривления поверхности стекла во время его колебания. Отраженный луч принимается оптическим приемником, размещаемым в точке приема отраженного луча. Изменения направления отраженного луча при колебаниях стекла вызывают соответствующие изменения положения пятна света на светочувствительном элементе (фотодиоде, фототранзисторе) оптического приемника. В результате этого изменяется освещенность светочувствительного элемента приемника и амплитудная модуляция электрического сигнала на выходе элемента. Сигнал после усиления прослушивается и записывается на аудиомагнитофон. Юстировка положения светочувствительного элемента оптического приемника производится по оценке оператором разборчивости речи.

Другой вариант построения системы лазерного подслушивания предусматривает реализацию в оптическом приемнике фазовой демодуляции путем сравнения фаз облучающего и отраженного лучей. С этой целью исходный луч с помощью полупрозрачного зеркала расщепляется на два луча. Одним из них облучается стекло, другой направляется к приемнику в качестве опорного сигнала. В оптическом приемнике создается электрический сигнал с уровнем, соответствующим разности фаз опорного и отраженного лучей или колебаний стекла окна. Этот вариант обеспечивает более высокую чувствительность системы подслушивания, но сложен в реализации.

Примером средства лазерного подслушивания является система РК-1035 фирмы PK Electronic. Система состоит из лазерных передатчика и приемника, магнитофона для записи перехваченной информации. Передатчик и приемник системы устанавливаются на треноге. Лазерный передатчик имеет размеры 65 × 250 мм, вес 1,6 кг, мощность — 5 мВт, длина волны излучения — 850 мкм. Лазерный приемник имеет размеры 65 × 260 мм, вес 1,5 кг. Электропитание — от сети и автономное.

Данные о возможностях систем лазерного подслушивания противоречивые. В рекламных материалах дальность указывается для разных систем от сотен метров до км. Однако без ссылки на уровень внешних акустических шумов эти величины можно рассматривать как потенциально достижимые в идеальных условиях. В городских условиях колебания внешнего стекла окна с двойным остеклением под действием шума улицы могут превышать амплитуду его колебания от акустического речевого сигнала. Следует также иметь в виду сложность практической установки излучателя и приемника, при которой обеспечивается попадание зеркально отраженного от стекла невидимого лазерного луча на фотоприемник. Оптимальный вариант применения — обеспечение перпендикулярности лазерного луча по отношению к поверхности облучаемого стекла. В этом случае отраженный луч вернется к фотоприемнику, установленному рядом (в одном помещении) с излучателем. Однако реализовать такой вариант можно лишь в редких случаях.

Уровни же диффузно отраженных от стекла лучей столь малы, что их не удается принять на фоне городских акустических шумов. Кроме того, следует отметить, что соотношение между стоимостью систем лазерного подслушивания и затрат на эффективную защиту от них не в пользу рассматриваемого метода добывания информации.

Следовательно, системы лазерного подслушивания, несмотря на их достаточно высокие гипотетические возможности, имеют ограниченное применение, в особенности разведкой коммерческих структур.

## 15.5. Средства высокочастотного навязывания

Добывание речевой информации путем высокочастотного навязывания достигается с помощью модуляции внешних высокочастотных радио- или электрического сигналов первичным электрическим сигналом, несущим речевую информацию. Для обеспечения такой модуляции необходимо дистанционно подавать внешнее электромагнитное поле или высокочастотные электрические сигналы на элементы, параметры которых или протекающие по ним токи меняются под действием речевых сигналов.

В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющие собой высокочастотные контуры с распределенными параметрами и объем которых меняется под действием акустической волны. Если частота такого контура совпадает с частотой высокочастотного навязывания, а поверхность полости находится под воздействием акустической информацией, то эквивалентный контур переизлучает и модулирует внешнее поле.

Более часто в качестве модулирующего применяется нелинейный элемент, в том числе в схеме телефонного аппарата. В этом случае высокочастотное навязывание обеспечивается подведением к телефонному аппарату высокочастотного гармонического сигнала путем подключения к телефонному кабелю высокочастотного генератора. В результате взаимодействия высокочастотного колебания с речевыми сигналами на нелинейных элементах телефонного аппарата происходит модуляция высокочастотного колебания. речевым низкочастотным сигналом и излучение промодулированного высокочастотного колебания проводами телефонного аппарата. Так как частота высокочатотного навязывания злоумышленнику известна, то модулированные высокочастотные сигналы могут быть перехвачены его приемником.

### Вопросы для самопроверки

1. Основные средства комплекса средств подслушивания.
2. Задачи, функции и состав акустического приемника.
3. Типы акустоэлектрических преобразователей для различных сред распространения.

4. Показатели акустического приемника.
5. Классификация микрофонов по принципу действия и направленности.
6. Характеристики микрофонов.
7. Отличия остронаправленных микрофонов от традиционных микрофонов.
8. Особенности диктофонов для скрытой записи речевой информации.
9. Преимущества и недостатки цифровых диктофонов по сравнению с лентопротяжными диктофонами.
10. Классификация закладных устройств.
11. Способы повышения скрытности закладных устройств.
12. Способы увеличения продолжительности работы закладных устройств.
13. Принципы работы средств лазерного подслушивания, ограничения при их применении.
14. Способы и средства высокочастотного навязывания.

# Глава 16. Средства скрытного наблюдения

## 16.1. Средства наблюдения в оптическом диапазоне

В оптическом видимом диапазоне света информация разведкой добывается путем визуального, визуально-оптического и телевизионного наблюдения, фото- и киносъемки, а в инфракрасном диапазоне — с использованием приборов ночного видения и тепловизоров.

Наибольшее количество признаков добывается в видимом диапазоне. Но видимый свет как носитель информации имеет малую проникающую способность, дальность его распространения в атмосфере сильно зависит от ее состояния, климатических и погодных условий. ИК-лучи как носители информации обладают большей проникающей способностью и позволяют наблюдать объекты при малой освещенности и даже в темноте. Но при их преобразовании в видимый свет для обеспечения возможности наблюдения объекта человеком происходит значительная потеря информации об объекте.

Так как физическая природа носителя информации в видимом и инфракрасном диапазонах одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имеют достаточно общую структуру. Ее можно представить в виде, приведенном на рис. 16.1.


*Рис. 16.1.* Структурная схема оптического приемника

Большинство средств наблюдения представляют собой оптический приемник, содержащий оптическую систему, светоэлектрический элемент, усилитель и индикатор. В зависимости от вида светочувствительного элемента оптические приборы делятся на

**визуально-оптические, фотографические** и **оптико-электронные**. В визуально-оптических средствах наблюдения светочувствительным элементом является сетчатка глаза человека, в традиционных фото- и киноаппаратах — фотопленка, а в оптико-электронных приборах — мишень светоэлектрического преобразователя (СЭП).

Оптическая система или объектив проецирует световой поток от объекта наблюдения на поверхность светочувствительного элемента (сетчатку глаза, фотопленку, фотодиод, фототранзистор, мишень СЭП). Светочувствительный элемент преобразует оптическое изображение в эквивалентное распределение плотности химического вещества или электронное изображение, количество «свободных» электронов каждой точки которого пропорционально яркости соответствующей точки оптического изображения. Способы визуализации изображения для разных типов оптического приемника могут существенно отличаться. Изображение в виде зрительного образа формируется в мозгу человека, на фотопленке — в результате химической обработки светочувствительного слоя, на экране технического средства — путем параллельного или последовательного съема электронов со светоэлектрического элемента, усиления электрических сигналов и формирования под их действием видимого изображения на экране оптического приемника.

Характеристики средств наблюдения определяются, прежде всего, параметрами оптической системы и светоэлектрического элемента, а также зависят от способов обработки электрических сигналов и формирования изображения при индикации. Основными характеристиками являются:

- диапазон длин волн световых лучей, воспринимаемых средством наблюдения;
- чувствительность;
- разрешающая способность;
- поле (угол) зрения и изображения;
- динамический диапазон интенсивности света на входе оптического приемника, не вызывающий искажение изображения на его выходе.

Средства наблюдения в зависимости от назначения создаются для видимого диапазона длин волн или его отдельных участков (зон), а также для различных участков инфракрасного диапазона.

**Чувствительность** средства наблюдения оценивается минимальным уровнем световой энергии, при которой обеспечивается требуемое качество изображения объекта наблюдения. Качество изображения зависит как от яркости и контрастности проецируемого изображения, так и от помех. Помехи создают лучи света, попадающие на вход приемника от других источников света, и тепловые шумы светоэлектрического преобразователя. На экране светочувствительного элемента при посторонней внешней засветке ухудшается контраст изображения аналогично варианту прямого попадания на экран телевизионного приемника или монитора компьютера яркого солнечного света.

**Разрешающая способность** характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные. Так как изображение формируется из точек (пикселей), размеры которых определяются разрешающей способностью средства наблюдения, то вероятность обнаружения и распознавания объекта возрастает с повышением разрешающей способности средства наблюдения (увеличением количества пикселей изображения объекта).

Размеры наблюдаемой части пространства характеризуются **полем** и **углом зрения**. Поле зрения — часть пространства, изображение которого проецируется на экран оптического приемника. Угол, под которым средство «видит» предметное пространство, называется **углом поля зрения**. Часть поля зрения, удовлетворяющего требованиям к качеству изображения по резкости, называется **полем** или, соответственно, **углом поля изображения**.

**Динамический диапазон** оптического приемника определяет в дБ интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения на выходе. Чем шире динамический диапазон оптического приемника, тем больше оперативные возможности его применения. Несоответствие динамического диапазона приемника диапазону силы света от объектов наблюдения приводит не только к искажению добываемой информации, но и может вызвать нарушение в работе приемника вплоть до разрушения светочувствительного элемента. Например, если человек посмотрит открытыми глазами на Солнце, то он в течение некоторого времени «слепнет».

Наиболее совершенным средством наблюдения в видимом диапазоне является зрительная система человека, включающая глаза и области мозга, осуществляющие обработку сигналов, поступающих с сетчатки глаз. Возможности зрения человека характеризуются следующими показателями:

- глаз воспринимает световые лучи в диапазоне 0,4–0,76 мкм, причем максимум его спектральной чувствительности в светлое время суток приходится на голубой цвет (0,51 мкм), в темноте — на зеленый (0,55 мкм);
- порог угловых размеров, которые глаз различает как две раздельные точки на объекте наблюдения, составляет днем 0,5–1 угл. мин, ночью — 30 угл. мин;
- порог контрастности различимого объекта по отношению к фону составляет днем 0,01–0,03, ночью — 0,6;
- диапазон освещенности объектов наблюдения, к которым адаптируется глаз, достигает 60–70 дБ;
- при освещенности менее 0,1 лк (в безоблачную лунную ночь) глаз перестает различать цвет;
- угловое поле зрения:
  - — в горизонтальной плоскости 65–95°;
  - — в вертикальной плоскости 60–90°;
  - — резкого изображения 30°;
- расстояние наилучшего зрения — 250 мм;
- время удержания взглядом изображения — 0,06 с.

Уникальные возможности зрительной системы человека обеспечиваются, прежде всего, оптической системой глаза, выполняющего функции объектива. Ее возможности и достигаются в результате того, что его кривизна с помощью специальных глазных мышц изменяется таким образом, чтобы обеспечить на сетчатке глаза максимально четкое изображение объектов, расположенных на различных расстояниях от наблюдателя. Хотя ведутся исследования по созданию подобных искусственных объективов, но приблизиться к возможностям глаза пока не удается.

### 16.1.1. Оптические системы

Основу оптических систем средств наблюдения составляют объективы, которые в силу постоянства сферической кривизны поверхностей линз и оптической плотности стекла проецируют изоб-

ражения с различного рода погрешностями. Наиболее заметны следующие из них:

- сферическая аберрация, проявляющаяся в отсутствии резкости изображения на всем поле зрения (оно резко в центре или по краям);
- астигматизм — отсутствие одновременной резкости на краях поля изображения для вертикальных и горизонтальных линий;
- дисторсия — искривление прямых линий на изображении;
- хроматическая аберрация — появление цветных окантовок на границах световых переходов изображения, вызванных различными коэффициентами преломления линзами объектива спектральных составляющих световых лучей.

С целью уменьшения погрешностей объективы выполняются из большого (до 10 и более) количества сферических линз с различной кривизной поверхностей. Все или отдельные группы линз склеиваются между собой. Аберрации линз существенно уменьшаются у асферических линз со сложной кривизной поверхности. Технология полировки асферических линз сложна и дорога. Выпускаются для недорогих объективов литые асферические линзы, уступающие по качеству стекла шлифованным сферическим линзам.

Возможности объективов описываются совокупностью характеристик, основными из которых являются:

- фокусное расстояние;
- угол поля зрения и изображения;
- светосила;
- разрешающая способность;
- частотно-контрастная характеристика.

**Фокусное расстояние** объектива представляет собой расстояние от оптической плоскости объектива до плоскости, где фокусируются входящие в объектив параллельные лучи света. По соотношению величины фокусного расстояния f объектива и длины диагонали кадра поля создаваемого им изображения d объективы делятся на короткофокусные, у которых $f < d$, нормальные или среднефокусные ($f \approx d$), длиннофокусные и телеобъективы с $f > d$, а также с переменным фокусным расстоянием. Фокусное расстояние глаза человека составляет около 17 мм. Значения фокусно-

го расстояния объективов унифицированы и принимают дискретные значения: 2,6, 3,5, 4,8, 6, 8, 12, 16, 25, 50, 75 мм и т. д.

Объектив с переменным фокусным расстоянием (панкратический) представляет собой сложную оптическую систему, в которой предусмотрена возможность смещения оптических компонентов вдоль оптической оси объектива, за счет чего изменяется величина фокусного расстояния. Величину фокусного расстояния изменяют **дискретно** или **плавно**. Дискретное изменение фокусного расстояния достигается применением **афокальных насадок**, уменьшающих или увеличивающих фокусное расстояние. Плавное изменение величины фокусного расстояния осуществляется перемещением отдельных линз объектива вдоль оптической оси по линейному или нелинейному закону. В зависимости от способа изменения эти объективы подразделяют на **вариообъективы** и **трансфокаторы**. Вариообъективы представляют собой единую оптическую схему, в которой изменение фокусного расстояния осуществляется непрерывным перемещением одной или нескольких линз вдоль оптической оси. Трансфокаторы состоят из насадки с переменным плавным увеличением и объектива с постоянным фокусным расстоянием.

Сложность оптической конструкции объективов с переменным фокусным расстоянием вызвана, прежде всего, тем, что при изменении фокусного расстояния должно автоматически сохраняться положение плоскости резкого изображения наблюдаемого объекта. Добиваются этого путем оптической или механической компенсации. В первом случае кратность изменения фокусного расстояния не более 3, во втором — 6–7.

По **углу поля зрения (изображения)** различают узкоугольные объективы, у которых величина этого угла не превышает 30°, среднеугольные (угол в пределах 30°–60°), широкоугольные с углом более 60° и, наконец, — с переменным углом поля изображения у объективов с переменным фокусным расстоянием.

Чем больше фокусное расстояние f объектива, тем больше масштаб изображения и больше деталей объекта можно рассмотреть на изображении, но тем меньше угол поля зрения. Поэтому для обнаружения объекта используют короткофокусные объективы, а для распознавания — длиннофокусные.

**Светосила** характеризует долю световой энергии, пропускаемой объективом к светочувствительному элементу. Очевидно, что чем выше светосила объектива, тем ярче изображение на светочувствительном элементе. На светосилу объектива влияют следующие факторы:

- относительное отверстие объектива;
- прозрачность (коэффициенты пропускания, поглощения, отражения) линз;
- масштаб изображения;
- коэффициент снижения яркости изображения к краю его поля.

Светосила без учета реальных потерь света в линзах вычисляется как квадрат относительного отверстия, равного $d/f$, где $d$ — диаметр входного отверстия (апертуры). Эффективное относительное отверстие объектива меньше геометрического на величину потерь света в его линзах. По величине относительного отверстия объективы делятся на **сверхсветосильные** с $d/f > 1/2$, **светосильные** с $d/f = 1/2{,}8–1/4$) и **малосветосильные** с $d/f \leq 1/5$ [5]. В зарубежной литературе в качестве характеристики светосилы объектива используют такой показатель, как «фокальное число» $F = f/d$. У человека с $f = 17$ мм и $d = 6$ мм $F = 2{,}8$, т. е. хрусталик глаза относится к светосильным объективам. Чем больше светосила объектива, тем выше чувствительность средства наблюдения. Однако при этом растут искажения изображения и для их уменьшения усложняют конструкцию светосильных объективов, что естественно приводит к их удорожанию. Для изменения относительного отверстия при чрезмерно большом диапазоне освещенности объекта наблюдения и повышения глубины резкости в объективе устанавливается механизм регулировки диаметра относительного отверстия — диафрагма. Величина диафрагмы изменяется вручную или автоматически.

Свет, падающий на линзу и проходящий через нее, отражается и поглощается. Количество поглощенного света зависит от толщины стекла (в среднем 1–2% на 1 см толщины). Линзы отражают 4–6% падающего на них света. Чем больше отражающих поверхностей имеет объектив, тем больше потери света. В объективах из 5–7 линз потери света на отражение могут составлять 40–50% [5]. Кроме того, свет, отраженный от внутренних поверхностей линз в

сторону плоскости изображения, накладывается на изображение и создает помеху в виде засветки изображения. Засветка уменьшает контраст изображения. Эти неблагоприятные факторы, возникающие в многолинзовых объективах, уменьшают просветлением линз.

**Просветлением** называется способ уменьшения переотражения света от внутренних поверхностей линз путем нанесения на них тонкой пленки. Толщина просветляющей пленки должна составлять 1/4 длины волны падающего на линзу света. Пленка сдвигает фазу отраженной от внутренней поверхности линзы волны на 180°, вследствие чего она компенсируется падающей волной. Первоначально объективы просветляли для узких участков спектра. Просветленный объектив в отраженном свете приобретал синефиолетовый оттенок и назывался «голубой» оптикой. Современные технологии просветления оптики позволяют наносить на поверхность линзы 12–14 слоев просветляющих пленок и перекрывать тем самым весь спектр видимого диапазона света. Такую оптику маркируют индексами МС — многослойное покрытие. Объективы МС в отраженном свете не меняют цвет.

Возможность объектива передавать мелкие детали изображения оценивается **разрешающей способностью**. Она выражается максимальным числом N штрихов и промежутков между ними на 1 мм поля изображения в его центре и по краям. Наиболее высокую разрешающую способность имеют объективы для микрофотографирования в микроэлектронике и линзы астрономических телескопов. Она достигает 1000 и более линий на мм. Изготовление таких объективов является чрезвычайно трудоемким процессом продолжительностью для линз телескопов большого диаметра в течение многих месяцев. Объективы с линзами из кварца, применяемые в фотографии, имеют существенно меньшее разрешение порядка 50 лин./мм, с штампованными из синтетических материалов линзами — еще ниже.

Так как одним из основных факторов, определяющих вероятность обнаружения и распознавания объектов, является контраст его изображения по отношению к фону, то важной характеристикой объектива как элемента средства наблюдения является **его частотно-контрастная характеристика**. Она служит мерой способ-

ности объектива передавать контраст деталей объекта и измеряется отношением контрастности деталей определенных размеров на изображении и на объекте. Уменьшение контраста мелких деталей на изображении вызвано тем, что в результате различных аберраций объектива на изображении размываются границы деталей наблюдаемых объектов.

Для количественной оценки частотно-контрастной характеристики в качестве исходного объекта используется эталонный объект наблюдения — мира в виде черно-белых линий с уменьшающейся шириной, нанесенных, например, тушью на белой бумаге. По результатам измерений контрастности n линий на проецируемом объективом изображении строится зависимость контраста K от количества линий n в одном мм. Зависимость K = f(n) определяет частотно-контрастную характеристику объектива.

В связи с большими техническими проблемами создания универсальных объективов с высокими значениями показателей, оптическая промышленность выпускает широкий набор специализированных объективов: для фото- и киносъемки, портретные, проекционные, для микрофотографирования и т. д.

Для добывания информации применяются объективы трех видов: для аэрофотосъемки, широкого применения (фото-, кино- и видеосъемки с использованием бытовых и профессиональных камер) и для скрытой съемки.

Объективы широкого применения разделяются в соответствии с размерами фотоаппаратов: для малоформатных и миниатюрных, среднеформатных и крупноформатных камер.

Для скрытого наблюдения используются:

- телеобъективы с большим фокусным расстоянием (300–4800 мм) для фотографирования на большом удалении от объекта наблюдения, например из окна противоположного дома и далее;
- так называемые точечные объективы для фотографирования из портфеля, часов, зажигалки, через щели и отверстия. Они имеют очень малые габариты и фокусное расстояние, но большой угол поля зрения.

Например, объектив фотоаппарата РК 420, вмонтированного в корпус наручных часов, имеет размеры 7,5 мм с апертурой 2,8 мм. В миникамерах фирм Hitachi, Sony, Philips, Ockar используются объективы диаметром 1–4 мм и длиной до 15 мм.

### 16.1.2. Визуально-оптические приборы

Для визуально-оптического наблюдения применяются оптические приборы, увеличивающие размеры изображения на сетчатке глаза. В результате этого повышается дальность наблюдения, вероятность обнаружения и распознавания мелких объектов. К визуально-оптическим приборам относятся **бинокли, монокуляры, подзорные трубы, специальные телескопы**. Для наблюдения за объектами наиболее распространены **бинокли**. Бинокль (от лат. bini —пара и oculus — глаз) — оптический прибор из двух параллельно соединенных между собой зрительных труб. В зависимости от оптической схемы зрительной трубы бинокли разделяются на **обыкновенные (галилеевские)** и **призменные**.

Зрительная труба призменного бинокля состоит из объектива, обращенного в сторону объекта наблюдения, системы призм, изменяющих направление распространения оптических лучей внутри бинокля и оборачивающих изображение, а также окуляра — объектива, обращенного к зрачку глаза. В обыкновенном бинокле призмы отсутствуют, оптические оси объектива и окуляра трубы совпадают, а расстояние между центрами объективов и центрами окуляров зрительных труб одинаковое и равно 65 мм — среднему расстоянию между зрачками глаз наблюдателя. Бинокли этого типа просты по устройству, обладают высокой светосилой, однако имеют малое поле зрения и не позволяют устанавливать углоизмерительную сетку в плоскости изображения. Наиболее распространены **призменные бинокли**. Они обладают сравнительно большим полем зрения и повышенной стереоскопичностью за счет увеличения расстояния между центрами объективов труб. В призменных биноклях устанавливают углоизмерительную сетку в фокальной плоскости окуляра. Зрительные трубы у призменных биноклей шарнирно закреплены на общей оси, что позволяет подбирать расстояние между окулярами по базе глаз наблюдателя (от 54 до 74 мм). Объективы и призмы оборачивающей системы закреплены в зрительных трубах неподвижно, а окуляры могут выдвигаться для обеспечения резкости изображения. Для этого на окулярных трубах наносятся диоптрийные шкалы.

Современные бинокли имеют большие коэффициенты (кратности) увеличения. Например, увеличение бинокля Б-15 равно 15,

а угол поля зрения — 4 град. Бинокль «Марк-1610» (США) имеет кратность увеличения 10 и 20 при угле зрения 5 и 2,5 град. соответственно.

При достаточно большом увеличении визуально-оптического прибора его угол зрения становится столь малым, что трудно из-за естественного дрожания рук (тремора) удерживать изображение наблюдаемого объекта в поле зрения прибора. Для стабилизации изображения визуально-оптические приборы устанавливают на штативе или треноге. В более дорогих приборах обеспечивают стабилизацию изображения при наблюдении с рук или с движущегося транспорта. Например, бинокль со стабилизацией изображения БС 16 × 40 имеет кратность увеличения 16, размеры 240 × 195 × 100 мм и вес не более 2,2 кг.

Чтобы улучшить наблюдение в тумане, при ярком солнечном освещении или зимой на фоне снега, на окуляры бинокля надеваются желто-зеленые светофильтры. В некоторых биноклях для обнаружения активных инфракрасных приборов ночью применяют специальный экран, чувствительный к инфракрасным лучам.

В последнее время применяются так называемые **панкратические бинокли**, плавно изменяющие увеличение в значительных пределах (с 4 до 20 и более). При этом в обратно пропорциональной зависимости изменяется величина угла поля зрения. Такие бинокли наиболее удобны для наблюдения, так как позволяют производить поиск объектов при большом угле поля зрения, но малом увеличении, а изучение объекта — при большом увеличении. Например, панкратический бинокль фирмы Tasko (США) имеет увеличение 8–15, угол зрения 6,0–3,6 градусов и диаметр входного зрачка 5–2,3 мм. У панкратических зрительных труб увеличение может изменяться в еще больших пределах. Например, кратность увеличения зрительной трубы фирмы Swiff (Великобритания) составляет 6–30 при угле зрения 7,5–1,3 градусов.

Для скрытного наблюдения удаленных объектов применяют **подзорные трубы** и **специальные телескопы**, имеющие объективы с большим фокусным расстоянием. Например, телескоп РК 6500 при фокусном расстоянии 3900 мм и диаметре входной апертуры 350 мм позволяет опознать автомобиль на удалении до 10 км. Однако телескоп имеет сравнительно большие размеры

460 × 560 × 1120 мм, вес 54 кг и устанавливается на специальном штативе с электроприводом.

На базе волоконно-оптических световодов созданы разнообразные типы **технических эндоскопов** для наблюдения через малые отверстия диаметром 4–10 мм. Технический эндоскоп представляет собой устройство для осмотра закрытых полостей и состоит из окулярной, основной и дистальной частей. Дистальная и основная части погружаются через отверстие или щель в закрытую от прямого наблюдения полость. Диаметр и длина погружаемой части эндоскопа составляют 7–10 мм и 1–2 м соответственно. Конструкция технического эндоскопа позволяет управлять поворотом дистальной части кабеля в горизонтальной и вертикальной плоскостях до ±90°. Угол поля зрения объектива дистальной части составляет 40–60°. Основная часть представляет собой жесткий, полужесткий или гибкий волоконно-оптический кабель. Наблюдение производится через окулярную часть. Система фокусирования объективов обеспечивает наблюдение резкого изображения объектов на удалении от 1 мм до более 5 м. Разрешающая способность технического эндоскопа — 5–17 лин/мм. Для освещения наблюдаемого пространства эндоскоп содержит осветительный жгут с галогенной лампой мощностью 20–150 Вт на конце, погружаемый с основной частью в закрытую полость и создающий в ней освещенность до 2000 лк.

### 16.1.3. Фото- и киноаппараты

Визуально-оптическое наблюдение, использующее такой совершенный оптический прибор, как глаз, является одним из наиболее эффективных способов добывания, прежде всего, информации о видовых признаках. Однако оно не позволяет регистрировать изображение для последующего изучения или документирования результатов наблюдения. Для этих целей применяют фотографирование и киносъемку с помощью фото- и киноаппаратов.

Традиционный **фотографический аппарат** представляет собой оптико-механический прибор для получения оптического изображения фотографируемого объекта на светочувствительном слое фотоматериала.

Все фотоаппараты состоят из светонепроницаемого корпуса с закрепленным на его передней стенке объективом, устройства для размещения или фиксации (транспортировки) светочувствительного материала, расположенного у задней стенки корпуса, и затвора.

Так как светочувствительный материал обеспечивает получение качественной фотографии при строго дозированной световой энергии, проецируемой на светочувствительный материал, то затвор пропускает в течение определенного времени (времени экспозиции, или выдержки) световой поток от фотографируемого объекта.

Указанные части фотоаппарата являются **основными**. По мере конструктивного развития фотоаппарат «обрастал» различными узлами и механизмами, которые облегчали и автоматизировали процесс съемки, позволяли расширить возможности применения фотоаппарата, улучшить его технические параметры. Эти узлы и механизмы называют **вспомогательными**. К ним относятся:

- видоискатель для определения границ поля изображения;
- фокусировочный механизм для совмещения фокальной плоскости объектива с плоскостью расположения светочувствительного материала;
- механизм, транспортирующий фотопленку на один кадр и устанавливающий ее точно против кадрового окна фотоаппарата;
- экспонометрический узел, предназначенный для определения экспозиционных параметров (выдержки и диафрагмы) в соответствии со светочувствительностью используемого фотоматериала и яркостью объекта;
- устройство искусственного освещения объекта съемки (фотовспышка).

Профессиональные фотоаппараты известных фирм (Nicon, Canon, Зенит, Kodak, Olympus, Contax, Pentax и др.) представляют собой сложнейшие оптико-электромеханические устройства, автоматически наводящиеся на «резкость» и учитывающие все изменения в освещенности объекта во время фотосъемки.

Размер используемого в них светочувствительных материалов положен в основу условного деления всех фотоаппаратов на несколько групп. По этому признаку (по размерам получаемых негативов) выделяют пять групп: **микроформатные, полуформат-**

**ные (мелкоформатные), мало-, средне- и крупноформатные.** Фотоаппараты применяют различные типы светочувствительных материалов: **фотопластинки, плоские и рулонные фотопленки.**

Другим важным признаком классификации является назначение фотоаппарата. По этому признаку они делятся на **общие** и **специальные**.

От способов обеспечения резкого изображения на светочувствительном материале (наводки на резкость) зависит конструктивное решение почти всего фотоаппарата. По этому признаку фотоаппараты можно разделить на следующие группы:

- с неподвижным жестко встроенным объективом, сфокусированным на гиперфокальное расстояние (до передней границы резко изображаемого пространства);
- с наводкой по монокулярному дальномерному устройству, механически связанному с объективом фотоаппарата;
- с наводкой на резкость по изображению на экране фотоаппарата (у так называемых зеркальных, или SLR-фотоаппаратов);
- автофокусирующие (с устройством автоматической фокусировки).

Устройства автоматической фокусировки изображения делят на активные (ультразвуковые, инфракрасные) и пассивные (сканирующие изображение, дальномерные, измеряющие контраст изображения). Исполнительным элементом устройства автофокуса является электродвигатель, который, перемещая объектив вдоль его оси, производит наводку на резкость.

По технической оснащенности фотоаппараты можно разделить на простые, средние и высокие.

По показателям оснащенности фотоаппарата встроенными экспонометрами, а также по степени автоматизации установки экспозиционных параметров фотоаппараты делят на три группы: с ручной установкой, с полуавтоматической и с автоматической установкой экспозиции.

Повышение технической оснащенности расширяет возможности фотоаппаратов, но усложняет возможность их миниатюризации.

Микроформатные фотоаппараты имеют более простую конструкцию и заряжаются узкой пленкой шириной 8–16 мм. Одна из

особенностей ряда ранних микроформатных фотоаппаратов — горизонтальная компоновка аппарата с объективом, утопленным в корпусе. Корпус таких моделей состоит из двух частей, одна из которых подвижная. Перед съемкой фотоаппарат телескопически раздвигается, открывая объектив и видоискатель. Одновременно производится транспортирование пленки и взвод затвора. Таким образом, выдвижная часть корпуса является одновременно защитным кожухом, рычагом взвода и протяжки пленки для следующего кадра («Минокс», «Агфаматик-4008», «Киев-30»).

Более новые модели имеют традиционную форму. Например, фотоаппарат «МФ-1» (Красногорский завод) представляет полуавтомат с пружинным приводом, имеет светосильный объектив с F2.8, размер кадра 18 × 24 мм. Конструкция фотоаппарата предполагает дистанционное управление, а пружинный привод дает возможность работать в любых климатических условиях. Недостаток — относительно большой шум при перемотке. Фотоаппарат «Robot-SC Electronic» менее шумный и при небольших габаритах работает с использованием стандартной пленки 35 мм. Для копирования документов наряду с мини- и микроформатными фотоаппаратами применяют специальные фотоаппараты. Например, копировальный фотоаппарат РК 320 состоит из зеркального аппарата, откидной стойки, источника освещения из двух ламп по 10 Вт, блока питания от батареи (8 × 1,5 В) и сети 220 В, а также из держателя документа. Устройство позволяет фотографировать документы размером А4–А6, размещается в портфеле-дипломате и весит 3,5 кг.

Возможности добывания информации путем фотографирования определяются как параметрами фотоаппаратов, так характеристиками (спектральным диапазоном, чувствительностью, разрешающей способностью) светочувствительных материалов, на которые проецируется объективом изображение наблюдаемого объекта.

**Светочувствительные материалы** (фото- и кинопленка, фотопластины, фотобумага) представляют собой подложку (прозрачную целлулоидную пленку, стеклянную пластину и плотную бумагу), на которую наносится тонкий слой из смеси желатина и светочувствительных веществ. Этот тонкий, сравнительно твердый и гибкий слой называется **эмульсией**. В качестве светочувствитель-

ных веществ наиболее широко применяются кристаллы галогенида серебра (AgBr, AgCl, AgJ). Галоидное серебро является непосредственным приемником световых лучей. Поэтому от особенностей строения, размеров, количества и пространственного распределения в слое зерен галоидного серебра существенно зависит качество получаемого изображения.

В момент экспонирования под действием квантов света в микрокристаллах галогенида серебра происходит образование металлического серебра, которое осаждается на центрах светочувствительности (центрах скрытого изображения), увеличивая их размер. Таким образом, в результате фотографирования в светочувствительном слое возникает скрытое изображение. Для превращения его в видимое изображение необходима химическая обработка светочувствительного слоя, включающая проявление, фиксирование, промывку и сушку.

При проявлении химические вещества проявителя восстанавливают экспонированные микрокристаллы галогенидов серебра до металлического серебра, в результате чего скрытое изображение становится видимым.

Микрокристаллы, не подвергшиеся действию света, остаются в светочувствительном слое. Для удаления из эмульсионного слоя неэкспонированных и, соответственно, не восстановленных в процессе проявления кристаллов галогенида серебра производится фиксирование, в ходе которого галогенид серебра под действием соответствующих химических веществ превращается в несветочувствительное легко растворимое соединение.

После промывки с целью удаления из светочувствительного слоя продуктов реакции проявления и фиксирования и последующей сушки получается негативное изображение.

В негативном изображении степень почернения его элемента пропорциональна яркости исходного изображения на светочувствительном слое. Для получения позитивного (прямого) изображения необходимо провести позитивный процесс, включающий фотопечать, проявление, фиксирование и сушку. Позитивная фотопечать проводится путем экспонирования фотоматериала через негатив. При проявлении позитивного фотоматериала на нем получается изображение, обратное по яркости изображению негатива.

Так как энергия фотонов снижается с увеличением длины волны, то для формирования требуемого спектрального диапазона светочувствительного материала в слой вводят добавки-сенсибилизаторы. Черно-белые фотопленки по спектральной чувствительности делятся на категории, указанные в табл. 16.1.

*Таблица 16.1*

| *Спектральная характеристика пленки* | *Зона сенсибилизации, мкм* | *Зона спектра, к которой чувствительна пленка* |
|---|---|---|
| Несенсибилизированная | До 0,50 | Ультрафиолетовая, фиолетовая, синяя |
| Ортохроматическая | 0,58 | Зеленая, желтая |
| Изоортохроматическая | 0,60 | Синяя, желтая, зеленая |
| Изохроматическая | 0,64 | Синяя, зеленая, оранжевая, оранжево-красная |
| Панхроматическая | 0,68–0,70 | Синяя, зеленая, красная |
| Изопанхроматическая | 0,70 | Синяя, зеленая, красная |
| Инфрахроматическая | 0,90 | Инфракрасная |

В настоящее время широко применяется, в особенности из космоса, «многозональная съемка», которая предусматривает одновременное (синхронное) фотографирование одного и того же участка земной поверхности или объекта в различных (обычно 4–6) узких (0,04–0,10 мкм) зонах спектра на фотопленки с различными спектральными характеристиками. Информативность многозональных снимков зависит от информативности зон спектра, в которых производят съемку. Но в любом случае она выше, чем черно-белых фотографий.

В современных способах цветной фотосъемки используются многослойные фотоматериалы, имеющие на одной подложке три эмульсионные слоя. Каждый из слоев чувствителен к лучам одного из основных цветов: синего, зеленого и красного. При съемке в каждом из трех эмульсионных слоев образуется скрытое изображение. Фотохимическая обработка цветных материалов сложнее, чем черно-белых, и состоит из следующих операций: проявление, отбеливание, фиксирование, промывка, сушка и ряда промежуточных операций, способствующих повышению качества цветного изображения. Отбеливание, отсутствующее при обработке чер-

но-белых материалов, предназначено для перевода металлического серебра, снижающего яркость красителей слоев, в его комплексную соль.

Многослойные цветные фотопленки существенно уступают черно-белым по разрешающей способности, что усугубляется также значительным влиянием воздушной дымки в атмосфере на контраст изображения в сине-фиолетовой зоне спектра. Но благодаря цвету цветные фотографии имеют высокую информативность.

В интересах разведки более распространена фотосъемка на основе спектрозональных аэрофотопленок, имеющих 2–3 эмульсионных светочувствительных слоя. В отличие от цветных пленок, к которым предъявляются требования по идентичности в колориметрическом отношении изображения и оригинала, на спектрозональных аэрофотопленках объекты отображаются в условных цветах, не соответствующих привычному цвету объектов.

Технология съемки и фотохимической обработки спектрозональной пленки не отличается от цветной. Но информативность спектрозональных снимков значительно выше, чем цветных, по следующим причинам:

- используются наиболее информативные с точки зрения возможностей обнаружения и распознавания объектов зоны спектра;
- зоны смещены в область больших значений длин волн, вследствие чего уменьшается отрицательное влияние воздушной дымки на контраст оптического изображения;
- двухслойные спектрозональные аэрофотопленки имеют более высокую (примерно в 2 раза) разрешающую способность, чем многослойные цветные пленки.

**Чувствительность фотоматериалов** измеряется в условных единицах ISO (ранее в ед. ГОСТа), в США и многих других странах — в единицах ASA, в Германии — в DINах. Перерасчет единиц светочувствительности, определенных по разным сенситометрическим системам, сложен, так как в каждой системе используются разные критерии светочувствительности. Система ISO практически идентична системе ASA. В единицах DIN чувствительность приблизительно равна увеличенному на 1 десятикратному значению десятичного логарифма значений светочувствительности в единицах ISO. Например, широко применяемая для бытовой

съемки пленка имеет чувствительность 100, 200 и 400 ед. ISO соответствует чувствительности 21, 24 и 27 ед. DIN соответственно. В зависимости от назначения чувствительность фотоматериалов колеблется в широком диапазоне — от единичных значений до тысяч. Фирма «Кодак» выпускает специальную фотопленку, значения чувствительности которой достигают 10 тысяч единиц. Такая пленка позволяет проводить фотосъемку при освещенности, оцениваемой человеком как темнота. Однако она требует специальной обработки за 10–12 часов перед фотосъемкой. Разработана монохроматическая пленка переменной чувствительности, величина которой зависит от длительности ее проявления.

**Разрешающая способность фотографических материалов**, так же как объективов, оценивается числом различимых линий на один мм. Способность фотоматериала раздельно с заданным контрастом воспроизводить мелкие близко расположенные детали изображения определяется его структурными свойствами. Зернистая структура фотографической эмульсии вызывает рассеяние света в слое при экспонировании и ограничивает возможность воспроизведения мелких деталей и резкость изображения. Причем чем выше чувствительность фотоматериала, тем больше зернистость эмульсии. Разрешающая способность фотопленок в зависимости от решаемых задач колеблется в широких пределах: от 80–100 лин/мм для любительской фотографии до единиц тысяч лин/мм для специальной фотосъемки малоподвижных и неподвижных объектов (в голографии, астрономии, микроэлектронике, полиграфии). Например, для получения высококачественных голографических изображений разрешающая способность пленок должна составлять около 5000 лин/мм. Разрешающая способность аэрофотопленки представляет собой компромисс между ее чувствительностью и четкостью изображения — 100–400 лин/мм. Высокая чувствительность аэрофотопленок необходима для уменьшения влияния так называемого «скоростного смаза», вызванного движением фотоаппарата со скоростью полета самолета относительно объекта съемки. Это явление приводит к размазыванию границ между двумя соседними градациями яркости и снижению в целом четкости изображения. Чем выше чувствительность пленки, тем меньше необходимое время экспонирования (выдержки) и меньше влияние «скоростного смаза».

С начала 90-х годов на основе достижений микроэлектроники развивается принципиально новое направление — цифровое фотографирование. **Цифровой фотоаппарат** представляет собой малогабаритную камеру на ПЗС-матрице, электрические сигналы с выхода которой записываются не на магнитную ленту, как в видеокамере, а преобразуются в цифровой вид и запоминаются полупроводниковой памятью фотоаппарата в виде специальных карт (CompastFlash, SmartMedia Card, MultiMedia).

Цифровой электронный фотоаппарат, обладая возможностями классического электромеханического фотоаппарата, предоставляет пользователю дополнительные функции, которые существенно повышают оперативность фотографии. К ним относятся: возможность съемки в непрерывном режиме с частотой 5–15 кадров/с, запись текстовых и звуковых комментариев, даты и времени фотосъемки, просмотр изображений в процессе и после съемки на поворачивающемся экране (LCD-панели размером 4–5 см), отображение текущих параметров съемки (числа отснятых кадров, объем свободной памяти, текущий режим компрессии) и др. Предусмотрены различные режимы просмотра кадров и стирание не понравившихся, печатание выбранных на фотопринтере. Цифровой фотоаппарат может иметь стандартный интерфейс для просмотра изображения на экране телевизора, записи на видеомагнитофон или печати на принтере.

Цифровой фотоаппарат также сопрягается с ПЭВМ. Отснятое изображение может отображаться на экране монитора, редактироваться с помощью графических редакторов, выводиться на печать, передаваться по сети.

Разрешение изображения цифрового фотоаппарата определяется разрешением его светоэлектрического преобразователя и составляет миллионы пикселей. Но с увеличением разрешения уменьшается при ограниченном объеме памяти количество кадров фотосъемки. Компромисс между разрешением и количеством кадров достигается введением возможности изменения оператором показателей разрешения запоминаемого кадра. С дополнительной памятью количество отснятых кадров может быть очень большим — сотни и в будущем тысячи.

Разрешение цифровых фотоаппаратов приближается к разрешению фотоаппаратов широкого применения, но уступает разрешению специальных фотопленок. Легко рассчитать, что кадр фото-

пленки стандартного размера 24 × 36 мм и разрешением 100 лин/мм содержит более 8,5 млн пикселей. Но для фотопленки с разрешением 500 лин/мм количество пикселей кадра возрастает до чрезвычайно большой величины — более 200 млн. Однако отсутствие у цифровых фотоаппаратов необходимости в химической обработке светочувствительных материалов, большая оперативность просмотра изображений в ходе фотосъемки и гибкость редактирования изображений на ПЭВМ делают их привлекательными не только для бытовой фотосъемки, но и для разведки. Учитывая перспективы миниатюризации радиоэлектронных элементов, прежде всего «памяти», и повышения разрешения ПЗС, у цифровых фотоаппаратов большое будущее.

Основными техническими характеристиками фотоаппаратов, влияющими на их возможности по скрытому фотографированию, являются:

- диапазон длин волн, формирующих видимое изображение;
- чувствительность;
- разрешающая способность;
- масса и размеры;
- бесшумность в работе.

Если диапазон длин волн определяется спектральной характеристикой светочувствительного элемента, то разрешение фотоприемника зависит как от разрешения светочувствительного элемента $R_ф$, так и разрешения объектива $R_о$. Из-за многочисленных погрешностей (аберраций) линзы обеспечить высокое разрешение объектива сложнее, чем светочувствительного элемента. Разрешающая способность типовых объективов любительских фотоаппаратов составляет около 50 лин/мм. Объективы профессиональных фотоаппаратов с более высоким разрешением представляют собой сложные оптические системы, стоимость которых выше, чем стоимость остальной части фотоаппарата. Разрешающая способность пары «объектив-фотопленка» $R_{оф}$ определяется по простой формуле: $R_{оф} = (R_ф R_о) / (R_ф + R_о)$.

Информация о движущихся объектах добывается путем кино- и видеосъемки с помощью киноаппаратов и видеокамер. При киносъемке изображение фиксируется на светочувствительной кинопленке, при видеозаписи — на магнитной пленке или в полупроводниковой памяти.

Под киносъемкой понимают процесс фиксации серии последовательных изображений (кадров) объекта наблюдения через заданные промежутки времени, определяемые частотой кадров в секунду. Каждый кадр кинофильма содержит изображение объекта в момент съемки. Число кадров колеблется от единиц кадров в минуту и даже часов для съемки медленно текущих процессов до сотен тысяч в секунду — для сверхскоростной специальной съемки, например для наблюдения электрического разряда или полета пули.

Устройство кинокамеры близко к устройству фотоаппарата с той принципиальной разницей, что в процессе киносъемки пленка скачкообразно продвигается с помощью грейферного механизма перед кинообъективом на один кадр. Закрытие объектива на время продвижения кинопленки осуществляется заслонкой (обтюратором), вращение которой перед объективом синхронизировано с работой грейфера. Киносъемка движущихся людей производится на 8- и 16-мм пленку с частотой 16–32 кадра в секунду.

### 16.1.4. Средства телевизионного наблюдения

Дистанционное наблюдение движущихся объектов осуществляется с помощью средств телевизионного наблюдения. Схема комплекса средств телевизионного наблюдения показана на рис. 16.2.

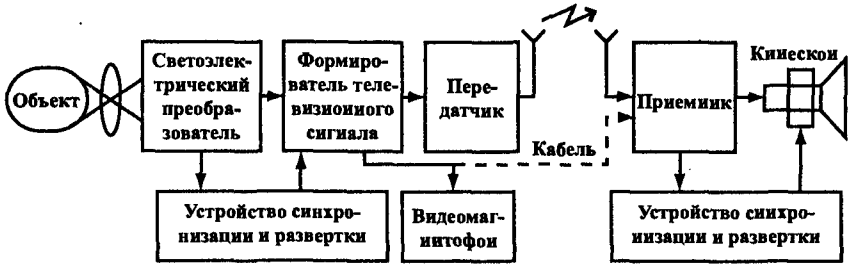



*Рис. 16.2.* Схема комплекса средств телевизионного наблюдения

При телевизионном наблюдении изображение объективом проецируется на светочувствительный слой фотокатода вакуумной передающей трубки или мишени твердотельного преобразователя. Фотокатод содержит вещества, из атомов которого кван-

ты световой энергии выбивают электроны, количество которых пропорционально энергии света (яркости элемента изображения). На фотокатоде образуется изображение Q(x,y,t) в виде электрических зарядов, эквивалентное оптическому B(x,y,t) изображению, где Q и B — значения соответственно величины зарядов и яркости в точках с координатами x и y в момент времени t.

В вакуумных телевизионных передающих трубках производится считывание величины заряда с помощью электронного луча трубки, отклоняемого по горизонтали и вертикали магнитными полями. Эти поля создаются отклоняющими катушками, надеваемыми на горловину телевизионной трубки.

За время развития телевидения разработано много типов передающих телевизионных трубок, отличающихся чувствительностью фотокатода и разрешающейся способностью. Появление достаточно простых ТВ-трубок типа «видикон» позволило создать компактные телекамеры. Миниатюрные видиконы с диаметром до 15 мм обеспечивают четкость 400–600 линий. На основе видикона разработаны различные варианты телевизионных передающих трубок: плюмбикон, кремникон, суперортикон, изокон и др., обеспечивающие качественное светоэлектрическое преобразование в широком диапазоне длин волн и освещенности.

В начале 70-х годов был открыт и реализован новый принцип построения безвакуумных твердотельных преобразователей «свет-электрический сигнал», т. н. **приборов с зарядовой связью (ПЗС)**. В основу таких приборов положены свойства структуры металл-окисел-полупроводник, называемой МОП-структурой (рис. 16.3).

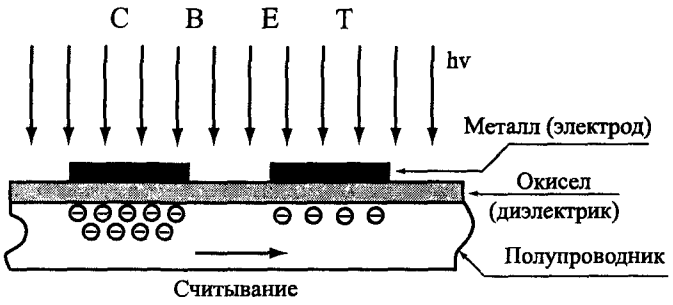



*Рис. 16.3.* Схема фрагмента ПЗС

Фотокатод или мишень ПЗС представляет линейку или матрицу из ячеек с МОП-структурами, образованную горизонтальными и вертикальными токопроводящими прозрачными электродами. Размеры каждой ячейки соответствуют размерам элемента изображения. Разрешающая способность ПЗС определяется количеством ячеек, размещающихся в поле изображения.

Считывание зарядов, образующихся в каждой ячейке ПЗС под действием света точек изображения, производится путем последовательного перекачивания зарядов с ячейки на ячейку под действием управляющих сигналов, подаваемых на электроды. В результате этого на выходе ПЗС образуется последовательность электрических сигналов, амплитуда которых соответствует величине заряда на ячейках мишени на ПЗС

Типовая **телевизионная передающая камера** содержит электронную плату с элементами электронной схемы, плату со светоэлектрическим преобразователем и объектив. В малогабаритной камере для скрытого наблюдения объектив и светоэлектрический преобразователь укрепляются на единой электронной плате.

Электронная схема электронной платы телевизионной камеры выполняет следующие функции:

- генерация сигналов управления светоэлектрическим преобразователем с целью считывания с него сигналов, эквивалентных яркости объектов изображения;
- усиление сигналов изображения с выхода светоэлектрического преобразователя;
- формирование сигналов (импульсов) синхронизации по строкам и кадрам изображения на экране монитора;
- формирование полного цветового сигнала, содержащего сигналы изображения, строчные и кадровые синхронизующие импульсы.

Светочувствительные матрицы современных телевизионных камер выполняются на приборах с зарядовой связью (ПЗС), которые по сравнению с вакуумными телевизионными передающими трубками имеют несоизмеримо малые размеры и энергопотребление. Размер светочувствительной области матрицы называется **оптическим форматом**. Для систем видеонаблюдения применяют форматы: 1/4, 1/3, 1/2, 2/3 и 1 дюйм. Следует отметить, что

размер диагонали матрицы меньше величины, равной произведению формата на эквивалент дюйма (2,54 мм). Например, размер матрицы 1/2" составляет 6,4 × 4,8 мм с диагональю 7,8 мм вместо 0,5 × 25,4 = 12,7 мм. Различие обусловлено тем, что размер ПЗС-матрицы определенного формата соответствует размеру поля изображения электронной передающей трубки диаметром, равному этому формату.

Чем больше формат матрицы, тем более высокое разрешение камеры можно обеспечить. Матрицы оптического формата 1/2, 2/3 и 1 дюйм применяют в камерах среднего и высокого класса, а 1/3 и 1/4 — в малогабаритных камерах и для скрытого наблюдения. На основе матриц формата 1/4 дюйма размером 3,4 × 2,4 мм компанией Watec (Япония) созданы сверхминиатюрные камеры WAT-660 (29 × 29 × 16 мм) и WAT-704R (цилиндрической формы диаметром 18 мм).

Для получения цветного изображения светочувствительный элемент ПЗС матрицы состоит из 3–4 светочувствительных ячеек, перед которыми установлены светофильтры красного, синего и зеленого цветов. В варианте 4 ячеек две из них чувствительны к зеленым лучам (перед ними установлены светофильтры зеленого света). Такой вариант приближает спектральную характеристику ПЗС матрицы к спектральной характеристике глаза, наиболее чувствительного к зеленому цвету. Из-за технологических и схемно-технических проблем и меньшей освещенности каждой ячейки элемента матрицы разрешение и чувствительность цветных камер хуже черно-белых. Для обеспечения высокого разрешения цветных камер световой поток от объектива с помощью призм направляют на 3 ПЗС-матрицы с соответствующими светофильтрами, что существенно усложняет конструкцию камеры. Камеры с ПЗС-матрицами называются также CCD-камерами.

**Объектив телевизионной камеры** может быть сменным и встроенным, с постоянным и переменным фокусным расстояниями. Основные характеристики объектива: **фокусное расстояние f** и **светосила**. Фокусное расстояние объектива определяет угол зрения телевизионной камеры. Объективы с малым фокусным расстоянием (около 2,8 мм) обеспечивают просмотр пространств большой площади, но получаемые изображения имеют мелкий масш-

таб. Кроме того, широкоугольные объективы вносят существенные искажения в изображение. Длиннофокусные объективы с f до 350 мм создают более четкое изображение, но с малой глубиной резкости. Для наблюдения за входной дверью, помещением, открытыми площадками применяются широкоугольные камеры с углом зрения 60–90°. Зависимость угла зрения объектива α и камеры от фокусного расстояния объектива f в мм описывается выражением $\alpha = \text{arctg}\,(h / 2f)$, где h — размер матрицы по горизонтали в мм. Следовательно, камеры с малым оптическим форматом имеют широкий угол зрения.

Возможности наблюдения с разными углами зрения создают вариообъективы (объективы с переменным фокусным расстоянием), фокусное расстояние которых может изменять ся вручную или сервоприводом.

Для скрытого наблюдения применяют миниатюрные телекамеры с объективами pin-hole (с «вынесенным входным зрачком») или специальные насадки. У объективов pin-hole плоскость апертуры диафрагмы совпадает с входным зрачком (см. рис. 16.4).

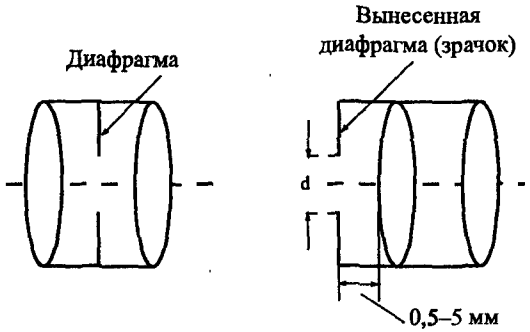



*Рис. 16.4.* Особенности объектива pin-hole

Такое расположение диафрагмы позволяет существенно уменьшить наружный диаметр d входного зрачка без заметного снижения светосилы объектива. Например, японская миниатюрная камера «WAT-660» имеет чувствительность 0,8 лк, разрешение 380 линий. При использовании объективов pin-hole с диаметром зрачка от 0,9 до 2 мм камеру можно встраивать в дверь, стену под обои,

настенные часы, в корпус извещателя и др. предметы. Для скрытого наблюдения через небольшое отверстие используется также насадка в виде оптоволоконного кабеля диаметром около 2 мм и длиною 50 см и более с объективом на конце.

В камерах со сменными объективами применяют два типа стандартных конструкций узлов присоединения:

- тип «С» («C-mount») с резьбой 2,54 × 0,8 и расстоянием до плоскости ПЗС матрицы 17,5 мм (старый стандарт);
- тип «CS» («CS-mount») с резьбой 2,54 × 0,8 и расстоянием до плоскости ПЗС матрицы 12,5 мм (новый стандарт).

Основными светоэлектрическими показателями камеры являются **разрешающая способность** и **чувствительность**.

**Разрешающая способность (разрешение)** телевизионной камеры определяется количеством телевизионных линий (ТВЛ), формирующих изображение. Телевизионные вещательные стандарты SECAM и PAL предусматривают разрешение 625 ТВЛ, NTSC (в США, Японии, Канаде и некоторых странах Латинской Америки) — 525 ТВЛ. Для телевизионных камер видеонаблюдения систем охраны требуемое разрешение ниже или выше в зависимости от решаемых задач. В будущем предполагается переход телевизионного вещания на формат высокой четкости с удвоенным разрешением.

Четкость изображения на экране монитора зависит не только от разрешения телевизионной камеры, но и от разрешения монитора и полосы пропускания линии связи камеры с монитором. Для безыскаженной передачи видеосигнала телевизионной камеры полоса пропускания линии связи должна быть не менее ширины спектра видеосигнала. Ширина спектра видеосигнала вещательного стандарта при разрешении 625 ТВЛ составляет 6,5 МГ, черно-белых камер систем охраны с разрешением 300 ТВЛ — 2,75 МГц и цветных — 3,8 МГц.

Способность телевизионной камеры работать при различной освещенности оценивается двумя показателями: **чувствительностью** и **минимальной освещенностью объекта наблюдения**.

**Чувствительность** камеры характеризуется минимальной освещенностью ПЗС-матрицы, при которой обеспечивается заданное качество изображения. Для получения изображения хорошего качества необходимо обеспечить отношение сигнал/шум на выходе

меры около 50 дБ. При отношении сигнал/шум около 30 дБ на экране монитора видны помехи в виде беспорядочных точек («снега»), минимально-допустимое отношение сигнал/шум — 20–24 дБ. В соответствии с этим минимально-допустимым отношением сигнал/шум определяется реальная чувствительность телевизионной камеры в отличие от предельной, когда размах сигнала равен размаху шумовой реализации. В этом случае на изображении практически, кроме шумов, ничего не видно. Реальная и предельная чувствительности телевизионной камеры различаются примерно в 10 раз. Обычной считается чувствительность порядка долей лк (для черно-белых камер) и единиц лк (для цветных). Телевизионные камеры высокой чувствительности работоспособны при освещенности порядка 0,01 лк.

Яркость изображения на ПЗС-матрице пропорциональна освещенности объекта наблюдения, коэффициенту отражения его поверхности и светосиле объектива. Поэтому при обозначении чувствительности камеры в единицах освещенности объекта наблюдения указывается кроме его освещенности также коэффициент отражения и F-число объектива. Обычно минимальная освещенность рассматривается для объектов с коэффициентом отражения 0,75 и объективов камеры с F = 1,4. При этих условиях освещенность ПЗС матрицы будет примерно в 10 раз меньше, чем объекта наблюдения.

Так как телевизионная камера обладает собственными шумами, то при уменьшении освещенности объекта снижается отношение сигнал/шум на выходе камеры. Повышение чувствительности телевизионной камеры, расширяющее возможности применения камеры для скрытого наблюдения, проводится по следующим направлениям:

- применение высокочувствительных ПЗС-матриц и светосильных объективов;
- применение электронно-оптических преобразователей-усилителей (ЭОП) яркости изображения;
- использование адаптивных режимов накопления и считывания заряда в ПЗС-матрицах.

Повышение чувствительности ПЗС-матриц достигается уменьшением потерь света из-за малой площади светочувствительных элементов, которые занимают только около 10% площади ПЗС-матрицы. Остальную часть ее площади занимают каналы пе-

реноса зарядов при их считывании. Применение микролинз перед поверхностью ПЗС-матрицы позволяет в 3–4 раза повысить чувствительность ПЗС-матрицы без линз. К другим мерам повышения чувствительности относится поиск материалов с более высокой чувствительностью в видимом диапазоне, с меньшим уровнем шума считывания, который уменьшает шумы видеосигнала, а также снижение влияния свечения транзисторов выходного устройства ПЗС-матрицы, создающей засветку изображения на ней.

Электронно-оптические преобразователи, применяемые в приборах ночного видения, усиливают в десятки тысяч раз свет от объекта наблюдения и позволяют приблизить чувствительность телевизионной камеры к чувствительности зрительной системы человека (около $10^{-4}$ лк). Их широкое использование сдерживается высокой стоимостью и низкой надежностью.

Для повышения чувствительности используется также возможность ПЗС-матрицы накапливать энергию светового сигнала между моментами считывания эквивалентных электрических сигналов. При накоплении n одинаковых сигналов отношение сигнал/шум увеличивается в $\sqrt{n}$ раз. ПЗС-матрицы с накоплением достигают чувствительности $(4–5)10^{-5}$ лк, т. е. позволяют наблюдать объекты в ночных условиях.

Телевизионная камера, так же как и фото- или кинокамера, содержит устройства, обеспечивающие требуемую выдержку и глубину резкости, а также устройства электронного преобразования видеосигнала, обеспечивающие повышение качества изображения. Основными такими устройствами являются **электронный затвор, автоматическая диафрагма, устройство автоматической регулировки усиления видеосигнала**.

**Электронный затвор** определяет время выдержки (длительность накопления зарядов ПЗС-приборами при проекции на них оптического изображения) электронным способом. Электронный затвор обеспечивает изменение выдержки от долей секунд до 1/100000 с, что позволяет наблюдать быстродвижущиеся объекты в широком диапазоне освещенности. Автоматический электронный затвор автоматически изменяет выдержку при изменении освещенности.

**Автоматическая диафрагма** изменяет относительное отверстие объектива в зависимости от освещенности объекта наблюде-

ния и требуемой глубины резкости, что особенно важно для обеспечения четкости изображений открытых площадок, коридоров и длинных помещений.

**Автоматическая регулировка усиления** в электронной схеме камеры поддерживает требуемый уровень сигнала на выходе видеоусилителя при изменении на 15–20 дБ и более уровня сигнала на выходе ПЗС матрицы — входе видеоусилителя.

Применяемая в видеоусилителе **гамма-коррекция (γ-коррекция) видеосигнала** улучшает качество изображения на экране приемной электронно-лучевой трубки. Необходимость коррекции вызвана нелинейной зависимостью яркости свечения люминофора экрана от амплитуды видеосигнала, которая аппроксимируется параболической функцией с показателем $\gamma = 2{,}2$. Гамма-коррекция предусматривает введение нелинейности коэффициента усиления видеоусилителя с $\gamma = 0{,}25–0{,}45$.

Яркость разных участков изображения может существенно отличаться, а автоматический затвор и устройство АРУ реагируют на усредненные значения яркости изображения. При попадании в поле зрения камеры, например, горящей электрической лампочки темные участки изображения становятся на экране монитора еще темнее, а яркие создают засветку изображения. В камерах с **компенсацией засветки («света сзади»)** опорная освещенность для автоматической установки выдержки и регулировки усиления оценивается по яркости центральной части изображения на ПЗС-матрице.

Электрический сигнал с выхода вакуумной передающей трубки или ПЗС усиливается и передается по кабелю или в виде радиосигналов к телевизионному приемнику. Последний выполняет обратные функции, преобразуя электрический сигнал в изображение, яркость каждого элемента которого эквивалентна амплитуде соответствующего сигнала. Формирование изображения производится на экране приемной масочной вакуумной трубки (кинескопа) или плоских панелей.

В вакуумной приемной телевизионной трубке (кинескопе) изображение создается на ее экране с люминофором электронным лучом, модулируемым электрическим сигналом изображения и отклоняемым по горизонтали (строке) и вертикали (по кадру) синхронно с траекторией отклонения луча передающей трубки или

считывания с ПЗС. Синхронность обеспечивается путем передачи синхронизирующих сигналов в виде групп импульсов, моменты формирования которых соответствуют границам строк и кадров. Синхроимпульсы совместно с сигналом изображения образуют полный телевизионный сигнал. В приемнике из полного телевизионного сигнала выделяются синхроимпульсы, которые синхронизируют работу устройств кадровой и строчной развертки. Эти устройства формируют сигналы, при прохождении которых по катушкам отклонения, надетым на горловину кинескопа, создаются магнитные поля, отклоняющие электронный луч.

Но вакуумные приемные телевизионные трубки громоздкие, тяжелые, хрупкие, нуждаются в высоковольтном (20–25 кВ) источнике постоянного тока, устройства развертки потребляют достаточно большую мощность, создаваемые трубкой поля, не безвредны для человека. Будущее за панелями.

Известно несколько типов плоских панелей для телевизионных приемников, но наиболее успешно развиваются **газоразрядные** и **жидкокристаллические панели**.

Газоразрядную панель образуют два плоскопараллельных стекла, между которыми размещены миниатюрные газоразрядные элементы. В инертном газе газоразрядного элемента под действием управляющих сигналов, формируемых микропроцессором устройства синхронизации и подаваемых на прозрачные электроды одного или обоих стекол, возникает разряд с ультрафиолетовым излучением. Это излучение вызывает свечение нанесенного на переднее или заднее стекло люминофора одного цвета черно-белой панели или люминофоров красного, зеленого или синего цветов цветной панели. Например, газоразрядная панель японской фирмы NHK имеет формат экрана 874 × 520 мм, 1075200 элементов с шагом 0,65 мм, толщину 6 мм и вес 8 кг. Газоразрядные панели имеют высокую яркость, позволяющую создавать контрастное изображение даже при солнечном свете.

Основой жидкокристаллической панели служат также две плоскопараллельные стеклянные пластины. На одну из них нанесены прозрачные горизонтальные и вертикальные токопроводящие электроды. В местах их пересечения укреплены пленочные транзисторы, два вывода которых соединены с электродами на стекле,

а третий образует обкладку конденсатора. Вторую пластину конденсатора представляет прозрачный металлизированный слой на второй стеклянной пластине, расположенной параллельно первой на расстоянии, измеряемом микронами. Между пластинами помещено органическое вещество (жидкий кристалл), поворачивающее под действием электрического поля угол поляризации проходящего через него света. С двух сторон панели укреплены поляроидные пленки, углы поляризации которых повернуты на 90° относительно друг друга.

Растр телевизионного изображения формируется сигналами, генерируемыми устройством синхронизации и подаваемыми на электроды стеклянных пластин. При подаче на эти электроды напряжения в точке их пересечения конденсатор заряжается и возникает электрическое поле между соответствующими обкладками конденсатора. В зависимости от величины напряжения изменяется угол поляризации жидкого кристалла между обкладками конденсатора. При отсутствии напряжения и, соответственно, электрического поля жидкий кристалл поворачивает угол поляризации света от лампы подсветки на 90°, в результате чего свет свободно проходит через поляроидные пленки. В зависимости от напряжения на обкладках конденсатора угол поляризации может изменяться от 90° до 0°, а прозрачность ячейки панели — от максимальной до непропускания света. Панель цветного телевизора содержит красный, зеленый и синий светофильтры, образующие триаду элемента разложения изображения.

Разрешение, яркость, контрастность жидкокристаллических мониторов приближаются к аналогичным характеристикам мониторов на электронно-лучевых трубках, ЖК-мониторы уступают по инерционности, но существенно превышают мониторы на электронно-лучевых трубках по масса-габаритным характеристикам, энергопотреблению и экологическим показателям.

Широкополосность аналогового телевизионного сигнала и большой объем значений пикселей цифрового телевидения создают проблемы при их консервации. При записи видеосигнала на магнитную ленту скорость перемещения ленты относительно записывающей головки видеомагнитофона должна составлять 5-6 м/с, что неприемлемо при реализации принципов записи, применяемых в аудиомагнитофонах.

В **видеомагнитофоне** реализован комплекс мер, обеспечивающих качество изображения, близкое к телевизионному, при приемлемых потребительских показателях видеомагнитофона и видеокассеты (габаритах, весе, времени записи на кассете). С этой целью сокращают полосу частот до 4–6 МГц, а для уменьшения линейной скорости перемещения магнитной ленты производится поперечно-строчная (поперек ленты) и наклонно-строчная (под острым углом к направлению движения ленты) запись видеосигналов на магнитную ленту с помощью вращающихся одной или нескольких (до 4) головок. Сигналы звукового сопровождения и управления записываются на боковых краях магнитной ленты.

Такие методы записи видеосигналов позволяют при сохранении высокой скорости движения ленты относительно головки значительно уменьшить ее продольную скорость и обеспечить приемлемое время записи на одной кассете. Для уменьшения влияния паразитной амплитудной модуляции из-за переменного контакта головки с лентой применяют частотную модуляцию с переменным индексом модуляции для разных частот и записывают на ленту частотно-модулированный сигнал. Кроме того, сохранение требуемых временных соотношений достигается применением высокоточного лентопротяжного механизма, систем автоматического регулирования электродвигателями и цифровых корректоров временных искажений.

Видеомагнитофоны с поперечно-строчной записью обеспечивают высокое качество изображения и звукового сопровождения, но они громоздкие и сложны в эксплуатации. Конструктивно более простыми являются профессиональные и бытовые видеомагнитофоны с наклонно-строчной записью.

В зависимости от требований к качеству записи и соответствующей скорости «лента-головка»» применяют ленты шириной 50,8, 25,4, 19, 12,65 мм и менее. Широкая лента используется в профессиональных видеомагнитофонах, 12,65 мм и менее — в бытовых Разнообразие значений ширины ленты в сочетании с разными способами записи обусловило множество форматов записи: для ленты шириной 50,6 мм — Q, 25,4 мм — B, C, 19,05 мм — U, 12,65 мм — L, M11, VHS, Beta и др. В бытовой видеозаписи наибольшее распространение получили форматы VHS и Beta. Видеофонограммы

формата VHS для отечественной бытовой аппаратуры имеют следующие параметры [6]:

- скорость головки относительно ленты — 4,85 м/с;
- продольная скорость ленты — 23,39 мм/с;
- ширина видеострочки — 0,04 мм;
- ширина дорожки звука — 0,3 мм;
- ширина дорожки управления — 0,75 мм;
- угол наклона строчки относительно края ленты — около 6 град.

Малая продольная скорость ленты позволяет на стандартной кассете с размерами 188 × 104 × 25 мм производить непрерывную запись изображения в течение 3–5 часов (в зависимости от толщины и длины ленты).

В целях повышения качества изображения развивается цифровая видеозапись в форматах D1–D5, а в интересах сокращения размеров и веса, что важно для решения задач по добыванию информации, — переход на малогабаритные кассеты. На базе широко применяемого формата VHS предложены форматы VHS-C (для кассеты с размерами 92 × 59 × 22,5 мм), S-VHC, Video 8 (95 × 62,5 × 15 мм, ширина ленты 8 мм) и малогабаритная кассета МК (102 × 63 × 12 мм с шириной ленты 3,8 мм). Формат S-VHC обеспечивает разрешение 440 ТВЛ вместо 330 для формата VHC. В современных видеомагнитофонах удается также снизить продольную скорость ленты до 1 см/с и менее с соответствующим увеличением времени записи. Например, в цифровом видеомагнитофоне EV-A80 (Sony) достигнута скорость ленты 0,6/0,3 см/с, время записи в формате V-8 — 540/1120 мин с разрешением 250 строк.

Аналоговые видеомагнитофоны постепенно заменяются на цифровые, в качестве вторичных носителей информации в которых используются жесткие диски или энергонезависимая память.

При существующих стандартах на параметры телевизионных средств наблюдения их разрешение на порядок хуже разрешения фотоснимков. Для повышения четкости изображения увеличивают в 2 раза разрешение и частоту кадров. Но при этом соответственно увеличивается ширина спектра телевизионного сигнала со всеми вытекающими из этого недостатками. Для уменьшения полосы изображение предварительно сжимают. Для телевизионного наблюдения в ИК-диапазоне применяют телевизионные камеры с ПЗС, чувствительными к ИК-лучам.

Для наблюдения в оптическом диапазоне применяют также лазеры, лучи которых в видимом или ИК-диапазонах подсвечивают объекты в условиях низкой естественной освещенности. Для этой цели луч лазера с помощью качающихся зеркал сканирует пространство с наблюдаемыми объектами, а отраженные от них сигналы принимаются фотоприемником так же, как при естественном освещении.

Видеопередатчики систем скрытого наблюдения работают в диапазоне частот от 60 МГц до 2,3 ГГц и выше. Их мощность составляет от 40 мВт до 50 Вт, при этом обеспечивается дальность передачи от нескольких метров до 20 км. Например, дальность передачи миниатюрного передатчика РК 5115 при мощности 1,5 Вт на частоте 236 МГц составляет 400 м. Для увеличения дальности передачи используются специальные ретрансляторы.

Для приема телевизионных радиосигналов используются как телевизионные приемники широкого применения, так и специальные. Например, аудио- и видеоприемник РК 625 обеспечивает прием аудио- и видео-сигналов в диапазоне от 60 МГц до 1,2 ГГц, а видеоприемник RX 100 — в диапазоне 1,2–2,3 ГГц. Видеоприемники имеют встроенные микропроцессоры, автоматизирующие операции по поиску и приему сигналов. Например, видеоприемник РК 6625 имеет 100 программируемых каналов памяти, 24-часовой таймер и автоматический режим поиска видеосигналов.

## 16.2. Средства наблюдения в инфракрасном диапазоне

Для визуально-оптического наблюдения в инфракрасном диапазоне необходимо переместить невидимое для глаз изображение в инфракрасном диапазоне (более 0,76 мкм) в видимый диапазон. Эта задача решается в приборах ночного видения (ПНВ) и тепловизорах.

Основу **приборов ночного видения** составляет электронно-оптический преобразователь (ЭОП), преобразующий невидимое глазом изображение объекта наблюдения в видимое. Самый простой ЭОП, так называемый стакан Холста (по имени изобретателя Холста де Бургоса) представляет собой стеклянный сосуд, из которого выкачан воздух (рис. 16.5).

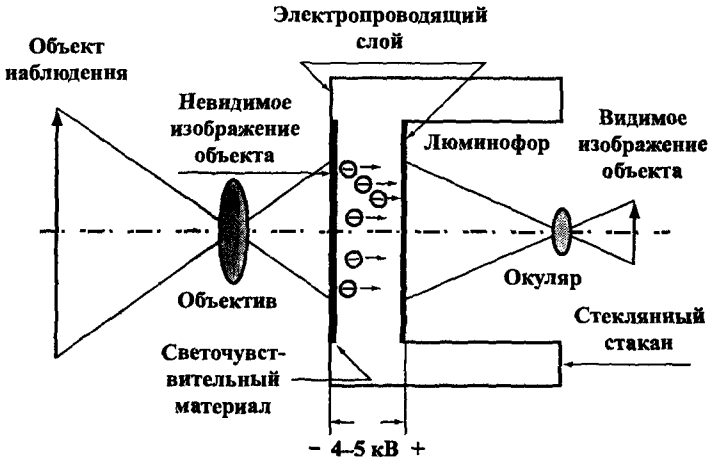



*Рис. 16.5.* Схема стакана Холста

Плоская поверхность стакана, обращенная к объекту наблюдения, металлизируется и на ней наносится светочувствительный материал из окиси серебра с цезием — фотокатод. Противоположная поверхность стакана представляет собой металлизированный экран с люминофором. К металлизированным поверхностям подводится достаточно высокое напряжение 4–5 кВ, в результате чего между ними возникает электрическое поле. На фотокатод объективом проецируется изображение в ИК-диапазоне. В каждой точке фотокатода под действием фотонов света возникают свободные электроны, количество которых пропорционально яркости соответствующей точки изображения. Электрическое поле вырывает свободные электроны из фотокатода и, разгоняя, устремляет их к экрану с люминофором. В моменты столкновения электронов с люминофором возникают вспышки видимого света, яркость которых пропорциональна количеству электронов. Таким образом на экране с люминофором формируется видимое изображение, близкое исходному в ИК-диапазоне.

Однако параметры (чувствительность, разрешение) рассмотренного ЭОП невысокие и не обеспечивают наблюдение при низкой освещенности и, следовательно, добывание демаскирующих признаков об объекте с мелкими деталями.

С момента создания в 1934 г. первого ЭОП в виде стакана Холста разработано несколько поколений этих приборов (от нулевого до 4-го), отличающиеся конструкцией и используемыми светочувствительными материалами. ЭОП 2-го и 3-го поколений, которые применяются в настоящее время, имеют чувствительный фотокатод, а между пластинами камеры размещается так называемая **микроканальная пластина**. Пластина содержит приблизительно 5000 микроканалов на 1 мм$^2$, внутри которых движутся электроны фотокатода. В результате устранения взаимного влияния электронов от соседних точек фотокатода, движущихся по разным микроканалам, достигается повышение разрешающей способности прибора ночного видения с микроканальной пластиной. Кроме того, в процессе движения электронов внутри каналов происходит «размножение» электронов в результате «выбивания» дополнительных электронов из стен каналов, покрытых специальными материалами. Основные усредненные показатели приборов ночного видения различных поколений приведены в табл. 16.2.

*Таблица 16.2*

| *Поколение* | *Максимальная чувствительность, мкА/лм* | *Коэффициент усиления* | *Разрешающая способность, лин/мм* | *Дальность распознавания фигуры человека при ЕНО* |
|---|---|---|---|---|
| 0 | 200 | 100–200 | 30 | 40 |
| I | 350 | 250–1000 | 40 | 60–110 |
| II | 1000 | $(2{,}5–3)10^4$ | 45 | 150–250 |
| III | 1350 | $(3–4)10^4$ | 50 | 250–300 |
| IV | 2000 | $10^5$ | 60 | 500 |

*Примечание.* Естественная ночная освещенность (ЕНО) соответствует $5 \cdot 10^{-3}$ лк.

На основе ЭОП 2-го и 3-го поколений созданы различные приборы ночного видения, включающие ночные бинокли и очки, артиллерийские приборы и прицелы для различных образцов военной техники. Самые малые по размерам ПНВ — очки на базе ЭОП 3-го поколения имеют угол зрения 40 град, дальность наблюдения (обнаружения) 500 м при естественном освещении около $10^{-3}$ лк, массу около 700 г.

Приборы ночного видения эффективно работают в условиях естественного ночного освещения, но не позволяют проводить наблюдения в полной темноте (при отсутствии внешнего источника света). Их чувствительность недостаточна для приема световых лучей в ИК-диапазоне, излучаемых телами.

Приборы ночного видения (ПНВ) разделяют на 3 группы:

- приборы малой дальности действия (ночные очки), позволяющие видеть фигуру человека на расстоянии 100–200 м. Вес и габариты этих приборов позволяют носить их в карманах, сумках, портфелях;
- приборы (ночные бинокли, трубы) средней дальности (человек виден до 300–400 м), наблюдение ведется с рук;
- приборы большой дальности действия (до 1000 м), устанавливаемые для наблюдения на треноге или подвижном носителе.

Например, прибор ночного видения — бинокль фирмы Noctron (США) имеет фокусное расстояние 135 мм, угол поля зрения — 10,6°, массу 1,98 кг, габариты 320 × 80 × 210 мм, дальность наблюдения человека 300–400 м.

Стационарный прибор ночного видения НМ-10С оснащается длиннофокусным объективом (F = 250 мм) с 10-кратным увеличением и специальным окуляром с переходными кольцами для подсоединения фото- и видеокамеры. Электронно-оптический преобразователь обеспечивает усиление 30000 и разрешение в центре 28 лин/мм. Прибор имеет габариты 200 × 600 мм, вес 5,1 кг и устанавливается на треноге.

По способу подсветки приборы ночного видения условно разделяют на три типа:

- объект наблюдения подсвечивается с помощью искусственного источника ИК-излучения, размещенного на приборе ночного видения;
- с подсветкой от естественного освещения;
- принимающего собственное тепловое излучение объекта наблюдения.

Приборы ночного видения первого типа содержат ИК-фару в виде обычного источника света мощностью 25–100 Вт, закрытого спереди специальным фильтром. Например, прибор ночного видения с подсветкой «Аргус» позволяет вести наблюдение в полной

темноте объектов на удалении до 120 м. На этом удалении мо
но различить силуэт человека и определить тип транспортно
средства. Опознать человека по признакам внешности и лица мо
но на значительно меньшем расстоянии — 35–50 м. Приборы но
ного видения при освещенности ночью в летнее время (приблизительно 0,005 лк) позволяют видеть фигуру человека на расстоянии до 300–400 м. Например, ПНВ отечественного производства «Ворон-3» имеет пороговый уровень освещенности для визуального обнаружения объектов 0,001 лк, для регистрации — 0,01 лк. Его разрешающая способность не менее 28 лин/мм, диапазон автоматической регулировки $10^5$ чувствительности, напряжение питания 5–9 В, масса — не более 1,2 кг.

Наблюдению объектов в полной темноте (при отсутствии внешних источников ИК-света) на рассмотренных принципах мешают тепловые шумы светоэлектрических преобразователей. Снижение уровня шумов достигается применением малошумящих светочувствительных материалов и охлаждением преобразователей. Для надежного обнаружения теплового излучения объекта наблюдения на фоне шумов светоэлектрического преобразователя (обеспечения отношения сигнал/шум более 1) последний нуждается в охлаждении до весьма низких температур — (–70 … – 200)°С.

Наблюдение объектов в свете собственных излучений (с точки зрения наблюдателя — в полной темное) обеспечивается в **тепловизорах** с охлаждаемыми светоэлектрическими преобразователями. Охлаждение производится с помощью термоэлектрических и микрокриогенных устройств до температуры порядка 70° К. В качестве светоэлектрических преобразователей применяются ИК-матрицы размером до 640 × 480 из пироэлектрических элементов и микроболометров, обеспечивающих опознавание человека на удалении до 1,5 км, а автомобиля — до 5 км. Масса современных тепловизоров составляет единицы кг. Например, японский тепловизор LATRO-S270 фирмы Nicon Corp. матрицей размером 537 × 505, охлаждаемой микрокриогенным устройством до температуры 77° К, имеет габариты 100 × 120 × 165 мм и массу 2,5 кг.

Основными характеристиками технических средств наблюдения в ИК-диапазоне, влияющими на их возможности, являются следующие:

- спектральный диапазон;

- пороговая чувствительность по температуре;
- фокусное расстояние объектива;
- диаметр входного отверстия объектива;
- угол поля зрения прибора;
- коэффициент преобразования (усиления) ЭОП;
- интегральная чувствительность.

## 16.3. Средства наблюдения в радиодиапазоне

Радиолокационное и радиотеплолокационное наблюдение осуществляется в радиодиапазоне электромагнитных волн с помощью способов и средств радиолокации и радиотеплолокации.

Для получения радиолокационного изображения в радиолокаторе формируется зондирующий узкий, сканирующий по горизонтали и вертикали, луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который, перемещаясь, синхронно с зондирующим лучом «рисует» на экране изображение объекта. Принципы радиолокационного наблюдения показаны на рис. 16.6.

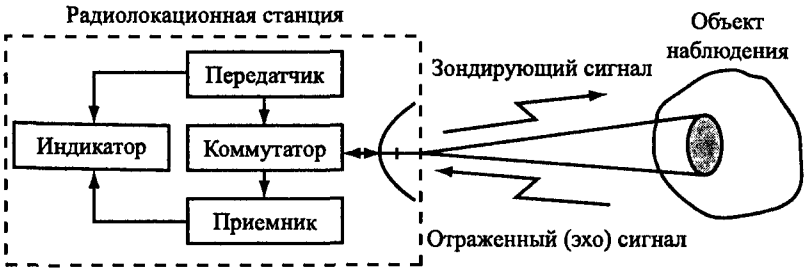



*Рис. 16.6.* Принципы радиолокационного наблюдения

Так как в радиолокаторе для передачи и приема используется одна и та же антенна, то при излучении коммутатор подключает к антенне передатчик, а при приеме — приемник. Момент излучения фиксируется на индикаторе РЛС в качестве точки отсчета для измерения дальности нахождения объекта. Расстояние до объекта равно половине пути, который проходит электромагнитная волна за время между моментами излучения зондирующего сигнала и приема отраженного от объекта сигнала.

Радиолокационное изображение существенно отличается от изображения в оптическом диапазоне. Различие обусловлено разными способами получения изображения и свойствами отражающей поверхности объектов в оптическом и радиодиапазонах.

Отражательная способность объекта в радиодиапазоне зависит не только от его геометрических размеров, но и от электропроводности его поверхности и конфигурации поверхности по отношению к направлению зондирующего луча радиолокатора. Если участок электропроводящей поверхности (металла, пленки воды) перпендикулярен направлению падающей на него электромагнитной волны радиолокационной станции, то большая часть ее энергии переотразится в сторону приемной антенны радиолокатора и будет визуализирована на его экране в виде яркой («блестящей») точки. При увеличении угла между зондирующим лучом и плоскостью участка поверхности объекта энергия поля у приемной антенны локатора будет уменьшаться вплоть до ее отсутствия. Следовательно, изображения на экране радиолокатора одного и того же объекта будут различаться при наблюдении его под разными углами. Отражающая способность объекта со сложной конфигурацией поверхности оценивается показателем, который называется **эффективной поверхностью рассеяния (ЭПР)**, измеряется в $м^2$ и обозначается символом $\sigma$.

Основными показателями радиолокационных средств наблюдения являются:

- дальность наблюдения;
- разрешающая способность на местности.

**Дальность радиолокационного наблюдения** зависит от излучаемой радиолокатором энергии (мощности передатчика локатора) и характеристик среды распространения электромагнитной волны. Ослабление электромагнитной волны зависит от дальности распространения и поглощения ее в среде. Чем короче длина волны, тем больше она затухает в атмосфере. Но одновременно тем выше может быть обеспечена разрешающая способность радиолокатора на местности.

**Разрешение радиолокатора** на местности определяется величиной пятна, которое создает луч радиолокационной станции на поверхности объекта или местности. Пятно тем меньше, чем

уже диаграмма направленности антенны радиолокатора. Ширина диаграммы направленности антенны, в свою очередь, обусловлена соотношением геометрических размеров конструкции антенны и длины волны. Кроме того, следует иметь в виду, что электромагнитная волна отражается от объекта или его деталей, если их размеры превышают длину волны. Если размеры их значительно меньше, то волна эти объекты огибает. В связи с этими соображениями наиболее широко в радиолокации применяется сантиметровый диапазон с тенденцией перехода в мм-диапазон.

Наземные радиолокаторы бывают малой, средней, большой дальности и сверхдальнего действия. РЛС малой дальности применяют для обнаружения людей и транспортных средств на расстоянии в сотни метров, средней — единицы км, большой — десятки км. Точность определения координат наземных РЛС составляет по дальности 10–20% и около градуса по азимуту.

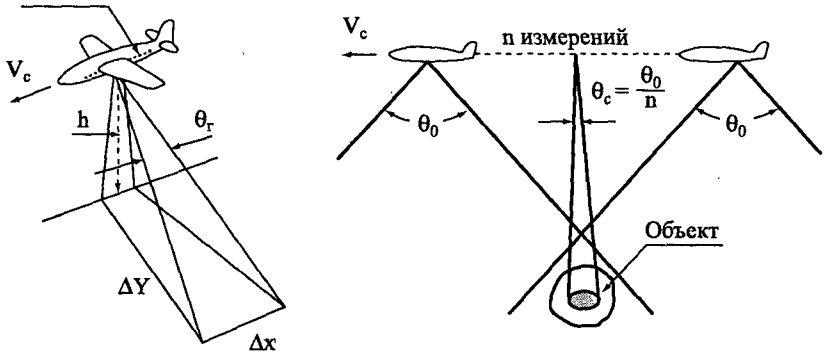
Сверхдальние (загоризонтные) РЛС используют эффект, открытый в 60-е годы Н. И. Кабановым. Этот эффект состоит в распространении радиоволн в декаметровом диапазоне на большие расстояния не только в прямом, но и обратном направлениях. Отражаясь от объектов на земной поверхности на удалении 800–4000 и более км от РЛС, электромагнитные волны, несущие информацию о демаскирующих признаках объектов, принимаются и регистрируются приемником радиолокатора. Но из-за нестабильности ионосферы разрешение таких РЛС значительно хуже, чем у надгоризонтных радиолокаторов.

Повышение разрешающей способности радиолокаторов без значительного увеличения размеров антенны, что особенно важно для воздушного и космического радиолокационного наблюдения, обеспечивается в **радиолокационных станциях бокового обзора (РЛС БО)**. Они размещаются на самолетах и разведывательных КА.

В РЛС БО применяются два вида антенн: **радиолокационные вдольфюзеляжные (РФА)** и **с синтезированной аппертурой (РСА)**.

Элементы антенны первого вида размещают на фюзеляже самолета с обеих его сторон или в подвесном контейнере-обтекателе. Благодаря такому расположению длина антенны может достигать

10–15 м. Такая антенна создает узкую (в доли градусов) диаграмму направленности в горизонтальной плоскости и широкую — в вертикальной. Антенна формирует один или два (при обзоре двух сторон) луча, направленных перпендикулярно линии полета самолета $V_c$ (см. рис. 16.7).




*а*) Вдольфюзеляжная антенна

*б*) Антенна с синтезированной апертурой

*Рис. 16.7.* Принципы работы радиолокатора бокового обзора

Излученный антенной РЛС БО радиоимпульс облучает участок местности шириной $\Delta x$ и длиной $\Delta y$. При полете самолета по прямолинейной траектории луч РЛС перемещается вместе с самолетом, а на индикаторе РЛС формируется изображение полосы местности, параллельной траектории полета самолета.

Особенностью бокового обзора является невозможность просмотра полосы местности под самолетом и ухудшение линейного разрешения пропорционально увеличению боковой дальности от самолета.

Повышение угловой разрешающей способности РЛС с синтезированной апертурой антенны основано на формировании узкой диаграммы направленности по азимуту с помощью виртуальной антенной решетки. В РЛС применяется небольшая антенна, широкая диаграмма направленности которой неподвижна относительно самолета и направлена на земную поверхность перпендикулярно линии полета. При полете самолета антенна РЛС последовательно занимает в пространстве положения на прямой траектории полета самолета, эквивалентные положениям элементов гипотетичес-

кой антенной решетки. В результате запоминания сигналов, последовательно принимаемых антенной в n точках траектории полета самолета, и их когерентного суммирования достигается эффект, аналогичный приему n элементами физической антенной решетки. Размер решетки (синтезированной апертуры) соответствует длине участка траектории, на котором производится запоминание и когерентное суммирование сигналов. Ширина диаграммы направленности в горизонтальной плоскости синтезированной антенны РЛС в n раз меньше ширины диаграммы физической антенны, установленной на самолете или КА. Используя этот метод, можно увеличить разрешающую способность РЛС по азимуту в 100 и более раз.

При наблюдении земной поверхности с помощью РЛС с РСА предъявляются жесткие требования к прямолинейности траектории полета самолета, к стабильности амплитудно-фазовых характеристик приемно-передающего тракта РЛС и устройств обработки сигналов, параметров среды распространения и характеристик отражения радиоволн наблюдаемыми объектами. Для цифровой обработки сигналов требуется также высокая производительность и большой объем памяти бортового компьютера.

Наряду с тенденцией уменьшения длины волны радиолокатора для повышения его разрешающей способности применяются РЛС в дециметровом и метровом диапазонах волн. Главное преимущество волн с более низкими частотами — существенное увеличение их проникающей способности. Для сухой почвы она может достигать нескольких метров. Это позволяет наблюдать сигналы, отраженные не только от поверхности Земли или объекта, но и различными неоднородностями в глубине. Появляются дополнительные демаскирующие признаки объектов и возможность их наблюдения при маскировке, например, естественной растительностью.

Эти свойства электромагнитной волны реализуются в радиолокационной станции **подповерхностной радиолокации**, называемой **георадаром**. Антенна георадара излучает сверхкороткие электромагнитные импульсы длительностью в доли и единицы наносекунды. Центральная частота и длительность импульса определяются исходя из необходимой глубины зондирования и разрешающей способности георадара. В диапазоне 0–500 МГц глубина зон-

дирования составляет единицы м, а разрешающая способность — десятки см. На более высоких частотах (около 1000 МГц) глубина зондирования уменьшается до долей м, но разрешающая способность увеличивается до единиц см. Георадары активно используются во многих сферах деятельности — в геологии, строительстве, экологии, оборонной промышленности и др., в том числе при поиске тайников, захоронений, подкопов.

Прием слабых тепловых радиоизлучений материальных тел (объектов) обеспечивает пассивная радиолокация или **радиотеплолокация**. Мощность излучения объектов в радиодиапазоне с приемлемой погрешностью определяется по формуле Релея—Джинса, в соответствии с которой энергетическая плотность (мощность в Вт на $м^2$) излучения пропорциональна температуре в °К и обратно пропорциональна квадрату длины волны.

**Радиотеплолокационное наблюдение** объектов осуществляется с помощью специальных радиоприемных средств, называемых **радиометрами**. В радиометре производится суммирование тепловых радиоизлучений элементов поверхности объекта наблюдения и усиление суммарного сигнала, его детектирование, усиление видеосигнала и формирование радиотеплолокационного изображения на индикаторе (экране) аналогично формированию изображения на индикаторе радиолокационной станции. В связи с тем что параметры антенны радиометра оказывают более существенное влияние на его дальность и разрешение, к антенне радиометра предъявляются более жесткие требования к максимуму коэффициента усиления и минимуму уровня боковых лепестков. Применяются зеркальные параболические, линзовые и многоэлементные антенны.

Для снижения собственных тепловых шумов во входных каскадах радиометра используются слабошумящие квантомеханические и параметрические усилители, различные способы компенсации помех в цепях радиометра и др.

Учитывая невысокие по сравнению с активной радиолокацией дальность и разрешение радиометров, возможности радиотеплолокации по добыванию видовых демаскирующих признаков весьма ограничены.

## Вопросы для самопроверки

1. Состав и технические характеристики типового оптического приемника.
2. Показатели объективов, влияющие на добывание информации.
3. Типы визуально-оптических приборов, используемых для добывания информации.
4. Назначение и состав технических эндоскопов.
5. Преимущества и недостатки цифровых аппаратов по сравнению с пленочными.
6. Принципы записи широкополосных сигналов на магнитную ленту.
7. Принципы работы приборов с зарядовой связью.
8. Принципы формирования изображений на газоразрядных и жидкокристаллических панелях. Их преимущества по сравнению электронно-лучевыми трубками.
9. Принципы работы приборов ночного видения и пути улучшения их параметров.
10. Отличия тепловизоров от приборов ночного видения.
11. Средства, применяемые для радиолокационного наблюдения с летательных и космических аппаратов, пути повышения их разрешающей способности.

# Глава 17. Средства перехвата сигналов

## 17.1. Средства перехвата радиосигналов

Перехват электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы добывания радио- и радиотехнической разведки. При перехвате решаются следующие основные задачи:

- поиск в пространстве и по частоте сигналов с нужной информацией;
- обнаружение и выделение сигналов, интересующих органы добывания;
- усиление сигналов и съем с них информации;
- анализ технических характеристик принимаемых сигналов;
- определение местонахождения (координат) источников представляющих интерес сигналов;
- обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

Упрощенная структура типового комплекса средств перехвата приведена на рис. 17.1.


*Рис. 17.1.* Структура комплекса средств перехвата радиосигналов

Типовой комплекс включает:

- приемные антенны;
- радиоприемник;
- анализатор технических характеристик сигналов;
- радиопеленгатор;
- регистрирующее устройство.

Антенна предназначена для пространственной селекции и преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствуют аналогичным характеристикам электромагнитной волны.

В радиоприемнике производится поиск и селекция радиосигналов по частоте, усиление и демодуляция (детектирование) выделенных сигналов, усиление и обработка демодулированных (первичных) сигналов: речевых, цифровых данных, видеосигналов и т. д.

Для анализа радиосигналов после частотной селекции и усиления они подаются на входы измерительной аппаратуры анализатора, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

Радиопеленгатор предназначен для определения направления на источник излучения (пеленг) или его координат.

Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

### 17.1.1. Антенны

Антенны представляют собой электромеханические конструкции из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования электрических сигналов в радиосигналы (для передающих антенн) и радиосигналов в электрические (для приемных антенн).

Возможности антенн, как приемных, так и передающих, определяются следующими электрическими характеристиками:

- диаграммой направленности и ее шириной;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

**Диаграмма направленности** представляет собой графическое изображение уровня излучаемого (принимаемого) сигнала от угла поворота антенны в горизонтальной и вертикальной плоскостях. Диаграммы изображаются в прямоугольных и полярных координатах (см. рис. 17.2).


*а*) Прямоугольные координаты *б*) Полярные координаты

*Рис. 17.2.* Диаграмма направленности антенн

Диаграммы направленности могут иметь разнообразный и изрезанный характер, определяемый механической конструкцией и электрическими параметрами. Лепесток диаграммы направленности с максимумом мощности излучаемого или принимаемого электромагнитного поля называется **главным** или **основным лепестком**, остальные — **боковыми** и **задними**. Соотношение между величинами мощности основного лепестка по сравнению с остальными характеризует направленные свойства антенны. Ширина главного лепестка диаграммы измеряется углом между прямыми, проведенными из начала полярных координат до значений диаграммы, соответствующих половине максимальной мощности излучения или 0,7 напряжения электрического сигнала приемной антенны. Чем меньше ширина диаграммы направленности антенны, тем выше ее коэффициент направленного действия.

**Коэффициент направленного действия (КНД)** определяет величину энергетического выигрыша, который обеспечивает направленная антенна по сравнению с ненаправленной.

Потери электрической энергии в антенне оцениваются **коэффициентом полезного действия (КПД)**, равного отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь.

Произведение этих двух коэффициентов определяет **коэффициент усиления** антенны (КУ). Так как КНД > 1, а КПД < 1, то коэффициент усиления в зависимости от значений сомножителей мо-

жет теоретически принимать значения как меньше, так и больше 1. Чем выше КУ, тем больший энергетический эффект обеспечивает антенна, но тем точнее необходимо ориентировать направление основного лепестка на источник излучения.

Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация которых представлена на рис. 17.3.

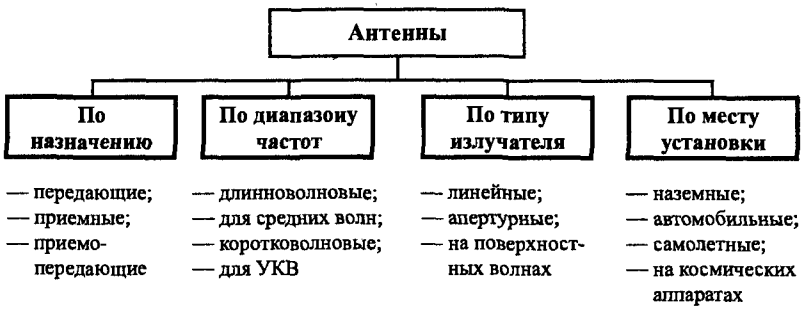



*Рис. 17.3.* Классификация антенн

Назначение передающих и приемных антенн ясно из их наименований. По своим основным электрическим параметрам они не различаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные, например антенны радиолокационных станций. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящимися под более высоким напряжением.

Эффективность антенн зависит от согласования размеров элементов антенны с длинами излучаемых или принимаемых волн. Минимальная длина согласованной с длиной волны электромагнитного колебания штыревой антенны близка к $\lambda / 4$, где $\lambda$ — длина рабочей волны. Размеры и конструкция антенн различаются как для различных диапазонов частот, так и внутри диапазонов.

Если для стационарных антенн требование к геометрическим размерам антенны может быть достаточно просто выполнено для коротких и ультракоротких волн, то для антенн, устанавливаемых

на мобильных средствах, оно неприемлемо. Например, рациональная длина антенны ($\lambda / 4$) для обеспечения связи на частоте 30 МГц составляет 2,5 м, что неудобно для пользователя. Поэтому применяют укороченные антенны, но при этом уменьшается их эффективность. По данным [7], укорочение длины этой антенны в 2 раза уменьшает эффективность до 60%, в 5 раз (до 50 см) — до 10%, а эффективность антенны, укороченной в 10 раз, составляет всего около 3% от рационального варианта.

По типу излучающих элементов антенны делятся на **линейные**, **апертурные** и **поверхностных волн**.

У линейных антенн поперечные размеры малы по сравнению с продольными и с длиной излучаемой волны. Линейные антенны выполняются из протяженных токопроводящих элементов (металлических стержней и проводов), вдоль которых распространяются токи высоких частот. В зависимости от величины нагрузки линии в ней возникают стоячие (линия разомкнута) или бегущие волны (сопротивление нагрузки равно волновому сопротивлению линии). По конструкции различают симметричные и несимметричные электрические вибраторы, бегущей волны, ромбические и рамочные антенны. В симметричном вибраторе провода линии — вибраторы разведены на 180° (рис. 17.4 *а*)).

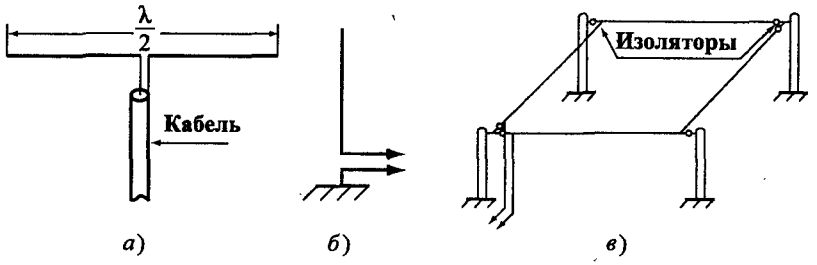



*Рис. 17.4.* Типы линейных антенн

Несимметричным вибратором называется одиночный линейный проводник, расположенный вертикально над проводящей поверхностью (корпусом, «землей») (рис. 17.4 *б*)).

Антенна бегущей волны, применяемая в коротковолновом диапазоне, представляет собой длинную двухпроводную линию с нагрузкой, равной волновому сопротивлению и к которой на одина-

новом расстоянии, не более 1/8 длины принимаемой волны, присоединены симметричные вибраторы. Ромбическая антенна имеет высокую направленность излучения и представляет собой длинную двухпроводную линию, провода которой расходятся у входа, а потом, образуя ромб, сходятся, замыкаясь на активное сопротивление, равное волновому сопротивлению линии. Рамочную антенну образуют один или несколько последовательно соединенных витков провода квадратной, круглой, треугольной формы, расположенных обычно в вертикальной плоскости (рис. 17.4 *в*)). Линейные антенны используются при ДВ, СВ, КВ и УКВ диапазонах длин волн. В ДВ, СВ и КВ диапазонах вибраторы укрепляют на мачтах, высота которых в ДВ диапазоне может достигать 100 и более метров.

Излучающим элементом **апертурных антенн** является их раскрыв. По виду апертуры различают **рупорные**, **линзовые**, **зеркальные** и **щелевые антенны** (рис. 17.5).

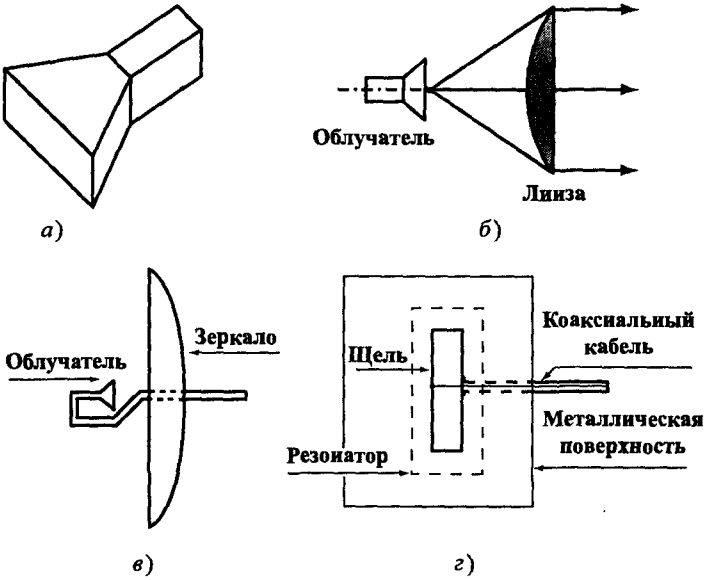



*Рис. 17.5.* Апертурные антенны

Так как для эффективного излучения размеры апертуры антенн должны быть соизмеримы с длиной волны, то эти антенны имеют приемлемые размеры в СВЧ диапазоне.

Рупорная антенна (рис. 17.5 *а*)) представляет собой конец волновода с рупором прямоугольной или круглой формы. По волноводу передается электромагнитная энергия от генератора передатчика, а рупор обеспечивает плавный переход от волновода к свободному пространству, уменьшающий отражение электромагнитной волны от конца волновода.

Основным элементом **линзовых антенн** (рис. 17.5 *б*)) является линза, принцип работы которой аналогичен оптической линзе. В передающей антенне линза преобразует расходящуюся от облучателя (рупор, конец волновода или вибратор) электромагнитную волну в плоскую волну. Приемная антенна фокусирует на облучатель падающую на раскрыв линзы электромагнитную волну. Линзы делятся на замедляющие, в которых фазовая скорость распространения электромагнитной волны ниже скорости света, и ускоряющие. Замедляющие линзы выполняются из диэлектрика, в который вкраплены токопроводящие элементы. Ускоряющие линзы изготовляются из параллельных металлических пластин или секций прямоугольных волноводов. Наиболее широко используются многолучевые линзы, обеспечивающие широкий сектор излучения и приема: сферические и цилиндрические линзы Люнеберга, линзы Ротмана и так называемые линзы R–2R.

Линзы, у которых электромагнитное поле в ее раскрыве формируется в результате отражения электромагнитной волны, излучаемой облучателем, от металлической поверхности специального рефлектора (зеркала), называются **зеркальными** (рис. 17.5 *в*)). Форма линзы в виде параболоида вращения, усеченного параболоида, параболического цилиндра или цилиндра специальной формы создает требуемую диаграмму направленности антенны. В диапазоне дециметровых и более длинных волн в качестве облучателя применяется вибратор, более коротких длин волн — волноводно-рупорные облучатели.

В линзовых антеннах путем увеличения размеров зеркала можно обеспечить высокое угловое разрешение. Они широко применяются в сантиметровом и дециметровом диапазонах волн, прежде всего для обеспечения космической связи и в радиоастрономии. Например, зеркало радиотелескопа РАТАН-600, работающего

в диапазоне 0,8–30 см, состоит из 895 щитов размерами 7,4 × 2 м$^2$, расположенных по кругу диаметром 600 м.

**Щелевая антенна** (рис. 17.5 *г*)) представляет собой металлический лист с щелью, облучаемый электромагнитным полем. В основном применяется узкая прямоугольная щель шириной (0,03–0,05)λ и длиной 0,5λ, но щель может быть иной формы, в виде угла, креста и др. В щели, расположенной перпендикулярно наводимым в листе токам, возбуждается электромагнитное поле. Для обеспечения односторонней направленности излучаемого поля щель с тыльной стороны закрывается резонатором в виде металлической коробки. Возбуждающий сигнал подводится к краям щели с помощью коаксиального кабеля непосредственно или с помощью зонда, укрепляемого внутри резонатора.

В антеннах поверхностных волн направленное излучение (прием) возникает в результате интерференции волн, излучаемых собственно возбудителем и распространяющихся с меньшей скоростью вдоль направителя поверхностной волны. В качестве возбудителей чаще всего используются односторонние направленные излучатели: рупор, открытый конец волновода, вибратор с рефлектором. Направители бывают **диэлектрические** (рис. 17.6) и **металлические**, а по форме — **плоские, дисковые** и **стержневые**.

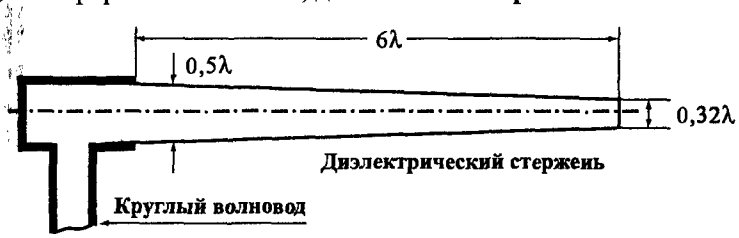



*Рис. 17.6.* Стержневая диэлектрическая антенна поверхностных волн

Для линейных антенн (например, вибраторов) коэффициент усиления (КУ) антенны характеризуется действующей высотой или длиной $h_a = E_a / E$, где $E_a$ — максимальное значение наводимой в антенне электродвижущей силы, E — напряженность электромагнитного поля в точке приема. Полоса частот, в пределах кото-

рых сохраняются заданные технические характеристики антенны, называется полосой ее пропускания.

Для параболической антенны коэффициент усиления антенны рассчитывается по формуле:

$$КУ = 4\pi S_{эф} / \lambda^2,$$

где $S_{эф}$ — эффективная площадь зеркала антенны; $\lambda$ — длина электромагнитной волны.

Создание антенн с высоким коэффициентом усиления и широкой полосой пропускания представляет основную проблему в области конструирования антенн. Чем выше КУ, тем труднее обеспечить широкополосность антенны. В зависимости от полосы пропускания антенны разделяются на **узкополосные**, **широкополосные**, **диапазонные** и **широкодиапазонные**.

Узкополосные антенны обеспечивают прием сигналов в диапазоне 10% от основной частоты. У широкополосных антенн эта величина увеличивается до 10–50%, у диапазонных антенн коэффициент перекрытия (отношение верхней частоты полосы пропускания антенны к нижней) составляет 1,5–4, а у широкодиапазонных антенн это отношение достигает значений в интервале 4–20 и более.

Совокупность однотипных антенн, расположенных определенным образом в пространстве, образует антенную решетку. Сигнал антенной решетки равен сумме сигналов от отдельных антенн. Различают линейные (одномерные) и плоские (двухмерные) антенные решетки. Антенные решетки, у которых можно регулировать фазы сигналов отдельных антенн, называют фазированными антенными решетками. Путем изменения фаз суммируемых сигналов можно менять диаграмму направленности в горизонтальной и вертикальной плоскостях и производить быстрый поиск сигнала по пространству и ориентацию приемной антенны на источник излучения.

### 17.1.2. Радиоприемники

Радиоприемник — основное техническое средство перехвата, осуществляющее поиск, селекцию, прием и обработку радиосигналов. В состав его входят устройства, выполняющие:

- перестройку частоты настройки приемника и селекцию (выделение) нужного радиосигнала;

- усиление выделенного сигнала;
- детектирование (съем информации);
- усиление видео- или низкочастотного первичного сигнала.

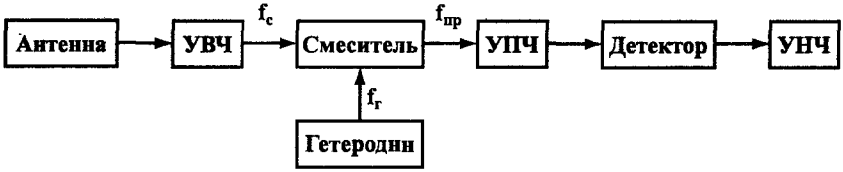
Различают два вида радиоприемников: прямого усиления и супергетеродинные. Появившиеся первыми приемники прямого усиления уступили супергетеродинным почти во всех радиодиапазонах, за исключением сверхвысоких частот. Такая тенденция объясняется более высокой селективностью и чувствительностью супергетеродинного радиоприемника по сравнению с приемником прямого усиления.

В **приемниках прямого усиления** сигнал на входе приемника (выходе антенны) селектируется и усиливается без изменения его частоты. Качество информации, снимаемой с этого сигнала, тем выше, чем меньше уровень помех (сигналов различной природы с частотами, близкими частоте настройки приемника). В идеале цепи селекции должны обеспечивать П-образную форму с полосой пропускания, равной ширине спектра принимаемого сигнала.

Такие фильтры имеют многозвенную, достаточно сложную конструкцию из тщательно настраиваемых многозвенных LC — элементов, или реализуются с использованием пьезоэлектрических и магнитострикционных эффектов (в пьезоэлектрических и электромеханических фильтрах).

Сложность проблемы обеспечения избирательности в радиоприемниках прямого усиления обусловлена техническими трудностями создания одновременно перестраиваемых по частоте узкополосных фильтров с высокими показателями по селективности, в особенности при их промышленном производстве. Только на сверхвысоких частотах удалось достигнуть высоких показателей по чувствительности и избирательности благодаря применению в широкополосных цепях высокой частоты специальных материалов и устройств: фильтров из железоиттриевого граната и малошумящих ламп бегущей волны.

В **супергетеродинном приемнике** проблема одновременного обеспечения высоких значений чувствительности и селективности решена путем преобразования принимаемого высокочастотного сигнала после его предварительной селекции и усиления в усилителе высокой частоты в сигнал постоянной частоты, называемой **промежуточной частотой** (рис. 17.7).




*Примечание*:
УВЧ — усилитель высокой частоты;
УПЧ — усилитель промежуточной частоты;
УНЧ — усилитель низкой частоты.

*Рис. 17.7.* Структурная схема супергетеродинного приемника

Усиление и селекция сигналов после преобразования выполняются на промежуточной частоте. Для постоянной промежуточной частоты задачи по обеспечению высокой избирательности и чувствительности решаются проще и лучше.

Преобразователь частоты состоит из гетеродина и смесителя. Гетеродин представляет собой перестраиваемый вручную или автоматически высокочастотный генератор гармонического колебания с частотой, отличающейся от частоты принимаемого сигнала на величину промежуточной частоты. Процесс преобразования частоты происходит в смесителе, основу которого составляет нелинейный элемент (полупроводниковый диод, транзистор, радиолампа). На него поступают принимаемый сигнал с частотой $f_c$ и гармонический сигнал гетеродина с частотой $f_г$. На выходе смесителя возникает множество комбинаций гармоник принимаемого сигнала и колебаний гетеродина, в том числе на промежуточной частоте $f_п = f_c - f_г$. Селективные фильтры усилителя промежуточной частоты пропускают только сигналы промежуточной частоты, которые усиливаются до величины, необходимой для нормальной работы детектора. В длинноволновом и средневолновом радиовещательном диапазонах $f_п = 465$ кГц, в УКВ — 10 МГц и более.

Однако супергетеродинному приемнику присущ ряд недостатков, вызванных процессом преобразования частоты. Основной из них состоит в том, что фильтры усилителя промежуточной частоты пропускают не только полезные сигналы, частота которых равна $f_c = f_г + f_п$, но и ложные с частотой $f_л = f_г - f_п$, симметричной («зеркальной») по отношению к частоте гетеродина $f_г$. Помехи на «зеркальной» частоте ослабляются путем двойного или даже

тройного преобразования частот в супергетеродинном приемнике. Промежуточная частота каждого последующего преобразования понижается. В результате этого первую промежуточную частоту можно без ущерба для избирательности приемника выбрать достаточно высокой. При больших значениях промежуточной частоты «зеркальная» частота существенно отличается от сигнала и подавляется входными фильтрами радиоприемника.

Возможности радиоприемника определяются следующими техническими характеристиками:

- диапазоном принимаемых частот;
- чувствительностью;
- избирательностью;
- динамическим диапазоном;
- качеством воспроизведения принимаемого сигнала (уровнями нелинейных и фазовых искажений);
- эксплуатационными параметрами.

**Диапазон принимаемых частот** обеспечивается шириной полосы пропускания селективных элементов входных фильтров и интервалом частот гетеродина. Настройка приемника на нужный диапазон или поддиапазон частот производится путем переключения элементов входных контуров и контура гетеродина, а настройка на частоту внутри диапазона (поддиапазона) — путем изменения частоты гетеродина. В радиоприемниках все шире в качестве гетеродина используется устройство — синтезатор частот, создающее множество (сетку) гармонических колебаний на стабилизированных фиксированных частотах с интервалом, соответствующих шагу настройки частоты приемника.

**Чувствительность радиоприемника** оценивается минимальной мощностью или напряжением сигнала на его входе, при которой уровень сигнала и отношение сигнал/шум на выходе приемника обеспечивают нормальную работу оконечных устройств (индикации и регистрации). Такая чувствительность называется реальной. Предельная чувствительность соответствует мощности (напряжения) входного сигнала, равного мощности (напряжению) шумов входных цепей радиоприемника. Информация полезного сигнала мощностью менее мощности шумов радиоприемника настолько сильно ими искажается, что передача информации воз-

можна только при кодировании ее специальными помехоустойчивыми кодами.

В диапазонах дециметровых и более коротких волн чувствительность измеряют в ваттах или децибелах по отношению к уровню в 1 мВт (дБм), в спектральной плотности в Вт/Гц или децибелах (по отношению к Вт/Гц), на метровых и более длинных — в микровольтах (мкВ). Реальная чувствительность современных профессиональных супергетеродинных приемников дециметровых и сантиметровых волн составляет $10^{-12}$–$10^{-15}$ Вт или –180 ... –200 дБ по отношению к Вт/Гц, приемников метровых и более длинных волн — 0,1–10 мкВ.

**Избирательность приемника** оценивается параметрами амплитудно-частотной характеристики (АЧХ) его селективных цепей, определяющей зависимость коэффициента усиления приемного тракта от частоты. Избирательность приемника максимальная, когда его амплитудно-частотная характеристика повторяет форму спектра принимаемого сигнала. В этом случае будут приняты все его спектральные составляющие, но не пропущены спектральные составляющие других сигналов (помех). Практически реализовать это требование чрезвычайно трудно, так как спектр сигналов с различной информацией имеет изрезанную постоянно меняющуюся форму и существуют большие технически проблемы при формировании амплитудно-частотной характеристики сложной заданной формы. В качестве идеальной АЧХ рассматривается П-образная форма с шириной, равной средней ширине спектра сигнала.

Избирательность реального приемника оценивается двумя основными показателями: шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника, реальная форма которой имеет колоколообразный вид.

Ширина полосы пропускания измеряется на уровне 0,7 по напряжению, а коэффициент прямоугольности оценивается отношением полосы пропускания на уровне 0,1 к полосе пропускания на уровне 0,7. Чем более пологой является АЧХ радиоприемника, тем шире полоса пропускания на уровне 0,1 по отношению к уровню 0,7 и тем больше величина коэффициента прямоугольности. Коэффициент пропускания позволяет количественно оценить пологий характер амплитудно-частотной характеристики радиопри-

емника. Чем ближе коэффициент прямоугольности АЧХ к 1, тем круче ее скаты и тем меньше помех «пролезет» по краям полосы пропускания. С целью уменьшения мощности помех, прошедших в тракт приемника, ширину его полосы пропускания устанавливают соответствующей ширине спектра сигнала. В приемниках для приема сигналов, существенно отличающихся по ширине, например речи и телеграфа, ширину полос пропускания различных селективных цепей изменяют путем коммутации селективных элементов (катушек индуктивности, конденсаторов).

Так как активные элементы усилительных каскадов радиоприемника (транзисторы, диоды и др.) имеют достаточно узкий интервал значений входных сигналов, при которых обеспечивается их линейное преобразование, то при обработке сигналов с амплитудой вне этих интервалов возникают их нелинейные искажения, в результате которых искажается информация. Возможность приемника обрабатывать с допустимым уровнем нелинейных искажений входные радиосигналы, отличающиеся по амплитуде, характеризуется **динамическим диапазоном**. Величина динамического диапазона оценивается отношением в децибелах максимального уровня к минимальному уровню принимаемого сигнала.

Для повышения динамического диапазона в современных радиоприемниках применяется устройство автоматической регулировки усиления (АРУ) приемного тракта, изменяющего его коэффициент усиления в соответствии с уровнем принимаемого сигнала.

Несоответствие амплитудно-частотной и фазовой характеристик, динамического диапазона радиоприемника текущим характеристикам сигнала приводят к его **частотным, фазовым** и **нелинейным искажениям** и потере информации.

Частотные искажения в радиоприемнике вызываются неодинаковыми изменениями составляющих спектра входного сигнала. Из-за частотных искажений сигнал на входе демодулятора искажается, что приводит к изменению содержащейся в нем информации.

Фазовые искажения сигнала возникают из-за нарушений фазовых соотношений между отдельными спектральными составляющими сигнала при прохождении его цепями тракта приемника.

Искажения, проявляющиеся в появлении в частотном спектре выходного сигнала дополнительных составляющих, отсутствующих во входном сигнале, называются нелинейными. Нелинейные искажения вызывают элементы радиоприемника, имеющие нелинейную зависимость между выходом и входом. Они возникают при превышении отношения значений максимального и минимального напряжений сигнала на входе приемника к его динамическому диапазону. Эти виды искажений приводят к изменению информационных параметров сигнала на входе демодулятора и, как следствие, к искажению информации после демодуляции.

Кроме указанных электрических характеристик возможности радиоприемников оцениваются также по их надежности, оперативности управления, видам электропитания и потребляемой мощности, масса-габаритным показателям.

Традиционные аналоговые радиоприемники постепенно вытесняются цифровыми, в которых сигнал преобразуется в цифровой вид с последующей его обработкой средствами вычислительной техники.

Большие возможности по перехвату радиосигналов в широком диапазоне частот предоставляют **сканирующие приемники**. Особенностями этих радиоприемников являются:

- очень быстрая (электронная) перестройка частоты настройки приемника в широком диапазоне частот;
- наличие устройств (блоков) «памяти», которая запоминает вводимые априори, а также в процессе поиска, частоты радиосигналов, не представляющие или, наоборот, представляющие интерес для оператора;
- информационно-техническое сопряжение на базе, как правило, интерфейса R-232S, приемника с компьютером, обеспечивающим возможность передачи сигналов в компьютер для их обработки и управления приемником.

«Память» сканирующего радиоприемника позволяет запоминать частоты обнаруженных радиосигналов и не тратить время на их анализ при последующем сканировании диапазона частот. В результате этого резко сокращается время просмотра широкого диапазона частот.

Во многих приемниках (AR-2700, AR-3000A, AR-5000, AR-8000, IC-R10, ICR-8500 и др.) предусмотрены интерфейсы сопряжения с

ПЭВМ, что позволяет автоматизировать поиск сигналов по задаваемым признакам, в том числе использующих простые виды технического закрытия.

На основе сканирующих приемников и ПЭВМ созданы **автоматизированные комплексы радиоконтроля** (радиомониторинга) помещений. Комплекс работает под управлением ПЭВМ, в реальном масштабе времени обеспечивает отображение на экране монитора амплитудно-частотных характеристик сигналов, их регистрацию на жесткий диск с возможностью последующей обработки. Ускоренный просмотр диапазона частот обеспечивается с помощью программно-аппаратных средств быстрого панорамного анализа (на основе быстрого преобразования Фурье).

Для перехвата радиосигналов со сложной структурой, применяемых в сотовой, пейджинговой и других видах мобильной связи, создаются специальные приемные комплексы.

Перехват наиболее информативных радиоизлучений усилителя и экрана монитора ПЭВМ возможен с помощью телевизионного приемника широкого применения с переделанными блоками строчной и кадровой синхронизации. Примером специального средства перехвата побочных излучений ПЭВМ в диапазоне частот 25–2000 МГц может служить комплекс 4625-COM-INT, который имеет 100 каналов памяти для накапливания перехваченной информации. После обработки информация восстанавливается в виде, отображаемом на экране монитора ПЭВМ. Комплекс обладает высокой чувствительностью (0,15 мкВ), имеет размеры 25 × 53 × 35 см и вес 18 кг. Следует отметить, что, хотя при перехвате радиоизлучений от иных источников побочных радиоизлучений ПЭВМ (системного блока, дисководов, принтера) не возникают серьезные проблемы, возможность добывания информации из перехваченных сигналов этих источников преувеличена. Достоверные факты о реализации такой потенциальной возможности отсутствуют.

### 17.1.3. Технические средства анализа сигналов

Технические средства измерения признаков сигнала включают большой набор различных программно-аппаратных устройств и приборов, в том числе устройства панорамного обзора и анализа спектра сигнала, селективные вольтметры, измерители времен-

ных параметров дискретных сигналов, определители видов модуляции кода и др.

Портативные анализаторы спектра при сравнительно небольших габаритах и весе (9,5–20 кг) позволяют принимать сигналы всех диапазонов частот (30 Гц–40 ГГц) и анализировать их тонкую структуру с высокой точностью. Погрешность измерения частоты сигнала составляет 15–210 Гц для частоты 1 Гц и 1–1,2 кГц — для частоты 10 ГГц, а погрешность измерения амплитуды сигнала 1–3 дБ. Например, цифровые анализаторы спектра HP8561E фирмы «Hewlett Packard» измеряют параметры сигнала в диапазоне частот 30 Гц–6,5 ГГц, а анализаторы спектра 2784 фирмы «Tektonix» — в диапазоне 9 кГц–40 ГГц.

Селективные микровольтметры позволяют измерять амплитуду с погрешностью 1 дБ и частоту с погрешностью 10–100 Гц в диапазоне частот до 1–2 ГГц. Характеристики некоторых из них приведены в табл. 17.1.

*Таблица 17.1*

| *Тип прибора* | *Диапазон частот, МГц* | *Чувствительность* |
|---|---|---|
| SMV-8 | 26–1000 | 1 мкВ |
| SMV-11 | 0,01–30 | 0,1 мкВ |
| STV-401 | 26–300 | 2 мкВ |
| ESH 2 | 0,009–30 | –30 дБ/мкВ |
| ESV | 20–1300 | –10 дБ/мкВ |

Высокоэффективными и компактными средствами технического анализа являются специальные приборы контроля радиосвязи (радиотестеры). К ним относятся «Stabilock 4015» (1,45–1000 МГц), «Stabilock 4032» (2–1000 МГц), HP 8920 A/D (0,4–1000 МГц) и др. Чувствительность указанных приборов не более 2 мкВ, а вес 13, 18,5 и 20 кг соответственно.

В составе радиотестера конструктивно объединены различные устройства приема и анализа сигналов: анализатор спектра, генератор сигналов, запоминающий осциллограф, устройства демодуляции и декодирования служебных сигналов, интерфейсы сопряжения с ПЭВМ и с принтером для регистрации результатов измерений.

### 17.1.4. Средства определения координат источников радиосигналов

Информативными признаками источника радиосигналов являются его координаты. Для определения координат применяется радиоприемник с поворачиваемой антенной, диаграмма направленности которой имеет острый максимум или минимум. Поворачивая антенну в направление достижения максимума (минимума) сигнала на выходе антенны, определяют направление на источник радиосигнала. Этот процесс называют **пеленгованием**, значения углов между направлениями на север и источник — пеленгами, а средство для пеленгования — радиопеленгатором, или пеленгатором.

Координаты источника радиоизлучений на местности рассчитываются по двум или более пеленгам из разных точек или по одному пеленгу и дальности от пеленгатора до источника. Для расчета координат источника радиоизлучений необходимы также координаты пеленгаторов.

Принципы пеленгования источника радиосигналов двумя пеленгаторами или одним подвижным из двух точек А и В иллюстрируются схемой на рис. 17.8.

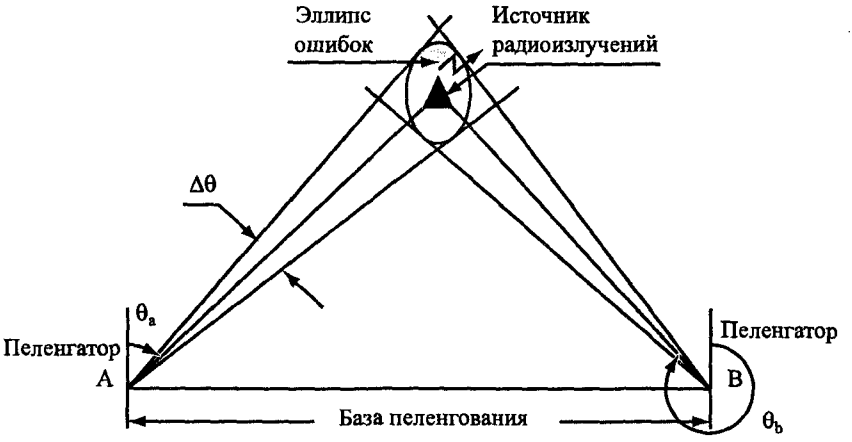



*Рис. 17.8.* Принципы пеленгования

Расстояние между двумя точками, из которых определяются пеленги, называется базой пеленгования. Координаты источника

соответствуют точке пересечения пеленгов на топографической карте или рассчитываются в результате решения триангуляционной задачи.

Инструментальные ошибки пеленгаторов, изменения условий распространения радиоволн, влияние объектов вблизи источников радиосигналов, отражения от которых искажают электромагнитное поле у антенн пеленгаторов, погрешности считывания пеленгов вызывают систематические и случайные ошибки пеленгования. Угловые ошибки пеленгования образуют эллипс ошибок (см. рис. 17.8), очерчивающий границы площади на местности, внутри которых находится источник радиоизлучений.

Для повышения точности координат применяют антенны пеленгаторов с большей крутизной изменения диаграммы направленности от угла поворота антенны, уменьшают систематические ошибки пеленгаторов и погрешности измерений, при расчетах учитывают условия распространения радиоволн от источника до пеленгаторов, увеличивают количество пеленгов. Более высокую точность пеленгования обеспечивают фазовые методы пеленгования на основе сравнения фаз, приходящихся от источника радиоволн на разнесенные в пространстве антенны пеленгаторов. Ошибки пеленгования измеряют в градусах, точность пеленгования — в процентах от дальности. Точность пеленгования в УКВ диапазонах на открытой местности составляет доли градусов: 0,1°, 0,2°; точность определения координат в этих диапазонах — доли процентов, в КВ-диапазоне — 3–5% от дальности. В городских условиях точность пеленгования ниже из-за влияния радиоволн, отраженных от зданий и автомобилей.

Процессы перехвата включают также регистрацию (запись, запоминание) сигналов с добытой информацией. Регистрация сигналов производится путем аудио- и видеозаписи, записи на магнитные ленту и диски, на оптические диски, на обычной, электрохимической, термочувствительной и светочувствительной бумаге, запоминания в устройствах полупроводниковой и других видов памяти, фотографирования изображений на экранах мониторов ПЭВМ, телевизионных приемников, осциллографов и спектроанализаторов.

## 17.2. Средства перехвата оптических и электрических сигналов

Добывание информации на носителях в виде электрических и оптических сигналов, распространяющихся по направляющим линиям (проводам и светопроводам), осуществляется путем съема сигналов с этих направляющих. Перехват производится **контактными** и **бесконтактными** способами. При контактном способе перехвата часть энергии сигнала отводится через физический контакт провода или светопровода приемника злоумышленника с проводом или светопроводом, по которым распространяется сигнал с информацией.

Подключение средства перехвата электрических сигналов к электрическим проводам кабеля может быть последовательным или параллельным (рис. 17.9 *а*) и 17.9 *б*)).

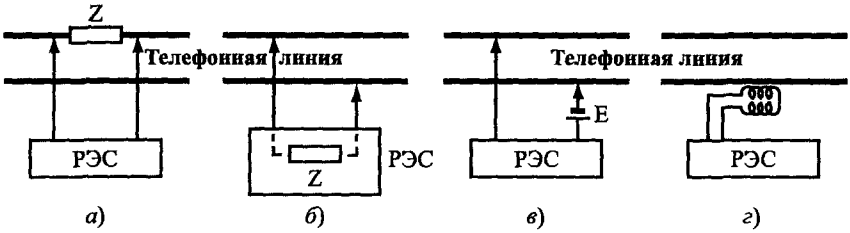



*Рис. 17.9.* Варианты подключения средств подслушивания (РЭС) к телефонной линии

При последовательном подключении в разрыв провода линии включается элемент приемника перехвата — сопротивление, сигнал с которого усиливается и воспроизводится в форме, доступной для человека, анализа или записи на аудио- или видеомагнитофон. При параллельном способе средство перехвата подключается к проводам линии параллельно. Наиболее простым средством перехвата сигнала с целью подслушивания речевой информации в телефонных линиях связи является телефонная трубка, которая подключается к проводам со снятой изоляцией телефонной линии с помощью контактов типа «крокодил». Последовательно или параллельно подключаемое средства перехвата можно представить в виде эквивалентного комплексного (активного и реактивного)

сопротивления Z. Поэтому контактное подключение уменьшает энергию сигнала и изменяет электрические параметры линии, к которой подключено средство перехвата. Эти изменения представляют собой демаскирующие признаки средства перехвата, по которым оно может быть обнаружено. Вероятность обнаружения зависит от величины изменения параметров линии и их стабильности.

Для снижения влияния подключенного средства перехвата уменьшают величину включенного последовательно сопротивления до единиц Ома или увеличивают входное сопротивление параллельно подключаемого средства до единиц МОма. Уменьшение напряжения в линии можно компенсировать подачей внешнего дополнительного напряжения E противоположного знака, как показано на рис. 17.9 *в*).

Современные средства защиты информации в проводных линиях позволяют обнаруживать последовательно включаемые средства с сопротивлением до 5 Ом и параллельно подключаемые — до 5 МОм. Кроме того, средство перехвата обнаруживается по изменению индуктивности и емкости линии за счет его индуктивности и емкости, а также по изменению волнового сопротивления линии.

Бесконтактные средства подключения — датчики перехватывают сигналы, которые излучают провода при протекании по ним электрического тока. В этом случае средства перехвата не отбирают у сигналов энергию и обнаруживаются существенно хуже. Вариант подключения бесконтактного дифференциального индуктивного датчика показан на рис. 17.9 *г*). В катушках датчика наводят ЭДС как поля, излучаемые токами в проводниках линии, так и других внешних полей. С целью компенсации одинаковых по уровню ЭДС внешних полей катушки включены встречно. За счет большей близости одной из катушек к проводу линии наводимая в ней ЭДС больше по величине, чем ЭДС в более удаленной от провода катушке. Чувствительность современных индуктивных устройств съема информации столь велика, что с их помощью удается снять информацию с бронированных кабелей.

Так как свет, распространяющийся в оптических кабелях, не выходит при соблюдении условий эксплуатации за пределы обо-

лочки, то перехват оптических сигналов возможен в двух вариантах:

- в местах входа (выхода) оптических сигналов в (из) кабеля;
- при деформации оптического кабеля, при которой угол его изгиба превышает угол предельного отражения лучей света в кабеле.

Первый вариант может быть реализован путем замены стандартных разъемов, соединяющих кабели со средствами или кабели друг с другом, на разъем с дополнительным отводом, к которому подключается оптический приемник злоумышленника. При добывании информации по второму варианту оптический кабель изгибается, поверхность места изгиба световолокна защищается от изоляции, и к нему прижимается светодиод. Хотя такой вариант теоретически возможен, практическая его реализация трудна из-за, прежде всего, сложностей в определении нужного тонкого световолокна среди множества других волокон оптического кабеля.

## Вопросы для самопроверки

1. Состав комплекса средств перехвата радиосигналов.
2. Основные характеристики антенн.
3. Классификация антенн по типу излучающих элементов.
4. Типы радиоприемников. Преимущества супергетеродинных радиоприемников как средства перехвата радиосигналов.
5. Параметры радиоприемников. Отличия предельной чувствительности от реальной чувствительности.
6. Особенности сканирующих радиоприемников.
7. Способы определения координат источников радиоизлучений.
8. Варианты подключения подслушивающих устройств к телефонной линии.
9. Способы добывания информации из световолокон.

# Глава 18. Средства добывания информации о радиоактивных веществах

Добыванием информации о радиоактивных веществах занимается радиационная разведка. Демаскирующими признаками радиоактивных веществ являются ионизирующие (радиоактивные) излучения (нейтронов, гамма-лучей, альфа- и бета-частиц — n, γ, α, β соответственно). Альфа-излучение (распад) представляет собой самопроизвольное превращение ядер, сопровождающееся испусканием со скоростью 14000–20000 км/с двух протонов и двух нейтронов, образующих ядро гелия. Бета-излучение представляет собой поток электронов, скорости которых близки к скорости света. Гамма-излучение является электромагнитным излучением с длиной волны менее 100 мкм. Заряд и кинетическую энергию α- и β-частиц определяют по их отклонению в электрическом и магнитном полях известной напряженности. Энергию и длину волны γ-излучения рассчитывают по энергии электронов, освобождаемых из различных веществ под действием этого излучения.

Для обнаружения и измерения радиоактивных излучений используют средства, реализующие **фотографический, сцинтилляционный, люминесцентный, химический** и **ионизационный методы**.

Основу **фотографического** метода составляет зависимость степени почернения фотоэмульсии от поглощенной энергии излучения. Под воздействием ионизирующих излучений молекулы бромистого серебра фотоэмульсии распадаются на бром и серебро. Кристаллы серебра вызывают почернение фотопленки при ее проявлении. По степени почернения определяют дозу излучения.

**Сцинтилляционные детекторы** представляют собой экран (пластину) из стекла, покрытый флюоресцирующим веществом (сульфидом цинка, антраценом или другими веществами), преобразующим кинетическую энергию радиоактивных частиц в энергию световой вспышки. Путем размещения за экраном фотоумножителя вспышки света преобразовываются в электрические сигналы с последующим измерением их интенсивности электронным счетчиком. Преимущество сцинтилляционного детектора состоит в том, что он может раздельно считать частицы, поступающие через очень короткие промежутки времени ($10^{-8}$–$10^{-9}$ с).

Дальнейшим развитием сцинтилляционного счетчика является **люминесцентная камера**, которая позволяет не только считать частицы в течение очень короткого времени ($10^{-13}$–$10^{-14}$ с), но и с помощью соответствующего электронно-оптического устройства регистрировать их траектории. В люминесцентных методах используется способность люминофоров накапливать поглощенную энергию излучения, а затем освобождать ее под действием дополнительного возбуждения при нагреве или облучении.

В **химических методах** используются свойства некоторых веществ изменять свою структуру под действием радиоактивного излучения. Например, при облучении хлороформа в воде образуется соляная кислота, изменяющая цвет добавленного в воду красителя. Изменением цвета реагирует на облучение трехвалентное железо с красителем. Зависимость изменения плотности цвета позволяет оценивать дозу поглощенного излучения.

Наиболее широко применяются **ионизационные методы** обнаружения радиоактивного излучения. Структура типового прибора радиационной разведки, реализующей эти методы, приведена на рис. 18.1.

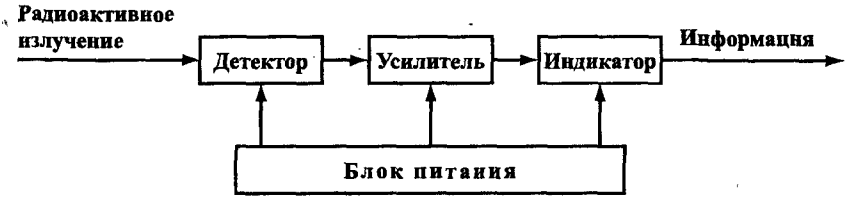



*Рис. 18.1.* Структурная схема прибора радиационной разведки

Детектор преобразует энергию радиоактивного излучения в электрические сигналы, которые после усиления поступают на стрелочный или цифровой индикатор. В качестве детектора используются **ионизационные камеры, газоразрядные счетчики, кристаллы полупроводника**.

**Ионизационные камеры** (Вильсона, пузырьковые, искровые) представляют собой сосуды цилиндрической или прямоугольной формы, заполненные газом с пересыщенным паром (в камере Вильсона), жидким водородом (в пузырьковой камере) и инертным газом (в искровой камере). В искровой камере имеются, кро-

ме того, плоскопараллельные близко расположенные друг к другу пластины, на которые подается высокое напряжение, чуть ниже пробойного. Когда через камеру Вильсона и пузырьковую камеру пролетает электрически заряженная частица, на возникающих на ее пути ионах конденсируются маленькие капельки жидкости, видимые при боковом освещении. При пролете быстрой частицы через искровую камеру вдоль ее траектории между пластинами проскакивают искры, создавая огненный трек.

В малогабаритных приборах радиационной разведки применяются в основном **газоразрядные счетчики** (счетчики Гейгера—Мюллера). Газоразрядные счетчики представляют собой герметичную стеклянную трубку, заполненную газовой смесью (аргона и воздуха, аргона и паров и др.) под давлением 0,1 атмосферы. Внутренняя поверхность трубки металлизирована. Внутри трубки протянута металлическая нить, на которую подается высокое положительное напряжение 1000–1500 В постоянного тока, а к металлизированной поверхности счетчика — отрицательное напряжение. Когда в газоразрядную трубку попадает ионизирующая частица, происходит лавинообразный процесс образования ионов, между электродами возникает короткий импульс тока, который подается на вход усилителя. В результате вторичной ионизации обеспечивается высокая чувствительность детектора. В простейшем варианте импульсы тока усиливаются и регистрируются в виде звуковых щелчков, в более совершенных дозиметрических приборах частота импульсов преобразуется в значение уровня излучения, отображаемое с помощью стрелочных или цифровых индикаторов.

Счетчики Гейгера—Мюллера для регистрации α-излучения имеют очень тонкое (0,002–0,003 мм) слюдяное (пленочное) окно, через которое частицы без существенного поглощения попадают в трубку. Для регистрации β-излучения окно трубки делают из алюминиевой фольги толщиной 0,1–0,2 мм, которая поглощает α-частицы. Трубки для регистрации γ-излучения закрыты слоем алюминия толщиной 1 мм, поглощающим α- и β-излучения.

Широкое распространение получили **кристаллические полупроводниковые детекторы**, основу которых составляют полупроводниковый кристалл кремния или германия с различными добав-

ками. Электропроводность кристалла изменяется под действием ионизирующего излучения.

Приборы для обнаружения и измерения радиоактивных излучений в зависимости от назначения делятся на **индикаторы радиоактивности, измерители мощности дозы (радиометры)** и **дозиметры**. По способу индикации интенсивности излучения — на стрелочные и цифровые.

Индикаторы радиоактивности информируют оператора световой или звуковой индикации о наличии в зоне поиска радиоактивных веществ, радиометры обнаруживают и измеряют уровень радиоактивного заражения среды, рентгенометры определяют мощность экспозиционной дозы, а дозиметры измеряют величину суммарной дозы, полученной за время пребывания в зоне радиоактивного заражения.

Для обнаружения и измерения радиоактивного заражения местности выпускаются разнообразные индикаторы радиоактивности, радиометры-рентгенометры со сменными фильтрами и дозиметры. Измерители мощности дозы делятся на стационарные, переносные и бортовые.

Для непрерывного контроля дозы, поглощаемой человеком, выпускаются **индивидуальные дозиметры**. Индивидуальный дозиметр ДКП-50А выполнен в форме авторучки из дюралевого корпуса, в котором расположены ионизационная камера с конденсатором, электроскоп, отчетное устройство и зарядная часть. В процессе зарядки конденсатора дозиметра под действием электростатического отталкивания отклоняется визирная нить электроскопа от внутреннего его электрода — пластины конденсатора. После заряда изображение нити на экране отсчетного устройства совпадает с нулем его шкалы отсчета. Под действием гамма-излучения за счет возникновения ионизационного тока уменьшается напряжение заряда центрального электрода, визирная нить приближается к центральному электроду, а ее изображение перемещается по шкале отсчетного устройства. Наблюдая через окуляр за положением изображения нити на шкале отсчета, можно в любой момент определить полученную экспозиционную дозу излучения. Этот дозиметр обеспечивает измерение индивидуальных экспозиционных доз гамма-излучения в диапазоне 2–50 Р при мощности экспозиционной дозы излучения 0,5–200 Р/ч.

Разнообразные профессиональные рентгенометры выпускает обнинское предприятие «Сигнал». Например, измеритель мощности дозы гамма-излучения ИМД-2 применяется в стационарных условиях, на летательных аппаратах, подвижных объектах и для пешей разведки. Индикация уровня производится с помощью светящегося сектора на шкале прибора. Он имеет следующие характеристики:

- диапазон измерения МЭД.....0 мкР/ч–1000 Р/ч;
- погрешности измерения ..... 30%;
- диапазон температур окружающей среды, °С .....–50 … +50;
- вес прибора, кг..... 1,6 кг;
- габариты, мм ..... 198 × 180 × 82.

Малогабаритные дозиметры (ДРС-01, ДКС-04, ДЭГ-8, ДРГ-01Т1, ДРГ-05М и др.) применяются людьми, имеющими дело с радиоактивными веществами, для измерения принятой ими дозы в течение определенного времени работы, например месяца. Пороговое значение дозы за год не должно превышать 5 бэр.

## Вопросы для самопроверки

1. Виды радиоактивных излучений, обнаруживаемых средствами добывания информации о радиоактивных веществах.
2. Методы обнаружения и измерения радиоактивных излучений.
3. Структура типового прибора радиационной разведки.
4. Типы приборов радиационной разведки.
5. Чем отличается экспозиционная доза от биологической?

# Глава 19. Система инженерно-технической защиты информации

## 19.1. Структура системы инженерно-технической защиты информации

Силы и средства, реализующие цели, задачи и методы инженерно-технической разведки, образуют систему инженерно-технической защиты информации. Любая сложная система имеет иерархическую структуру. Первый уровень структуры образуют подсистемы, ниже — комплексы, еще ниже — подкомплексы. Каждый структурный элемент объединяет силы и средства, решающие определенные задачи системы. В соответствии с рассмотренными методами в состав системы должны входить подсистемы физической защиты информации и подсистема защиты информации от утечки (рис. 19.1).


*Рис. 19.1.* Структура системы инженерно-технической защиты информации

**Подсистема физической защиты источников информации** включает силы и средства, предотвращающие проникновение к

источникам защищаемой информации злоумышленника и стихийных сил природы, прежде всего пожара. Ее основу составляют комплексы инженерной защиты источников информации и их технической охраны. Инженерные конструкции создают преграды, которые задерживают источники угрозы на пути их движения (распространения) к источникам информации. Однако для обеспечения защиты информации необходимо нейтрализовать угрозы раньше времени воздействия злоумышленника и стихийных сил на источник с защищаемой информацией. Для этого, как отмечалось во 2-м разделе, угроза должна быть обнаружена и предотвращена силами и средствами нейтрализации. Эти задачи решаются силами и средствами комплекса технической охраны источников информации. Следовательно, для эффективной физической защиты информации необходимо обеспечить высокую вероятность обнаружения источников угроз воздействия, задержку этих источников на время, превышающее время прибытия к месту проникновения и срабатывания сил и средств нейтрализации угроз.

Так как физическая защита источников информации не отличается от физической защиты других материальных ценностей и людей, то эта подсистема имеет универсальный характер и создается там, где возникает потребность в защите любых материальных ценностей.

**Подсистема защиты информации от утечки** является специфичным образованием, необходимым для защиты информации, и предназначена для выявления технических каналов утечки информации и противодействия ее утечке по этим каналам.

Каналы утечки информации, так же как любые другие объекты, обнаруживаются по их демаскирующим признакам. Прямыми признаками канала являются характеристики его элементов, которые создают предпосылки для утечки информации. В отличие от признаков злоумышленников и стихии признаки носителей информации в каналах утечки информации трудно обнаруживаются техническими датчиками. Например, опасные сигналы, создаваемые ПЭМИН, имеют столь малую мощность, что обнаруживаются в ходе специальных проверок с использованием дорогостоящей измерительной аппаратуры. Поэтому основные признаки, по которым обнаруживаются каналы утечки, — косвенные. Так как кос-

венные признаки, как правило, менее информативные, то для выявления по ним каналов утечки и оценки их угроз необходимо проведение анализа данных специалистами с достаточно высоким уровнем подготовки.

Неопределенность видов и времени проявления угроз информации, большое количество и разнообразие средств ее защиты, дефицит времени в случаях чрезвычайных ситуаций предъявляют повышенные требования к управлению элементами системы инженерно-технической защиты информации. Элементы управления образуют **комплекс управления**. Он должен обеспечить:

- реализацию общих принципов защиты информации;
- согласование в рамках единой системы функционирования подсистемы физической защиты информации и подсистемы защиты ее от утечки;
- оперативное принятие решений по защите информации;
- контроль эффективности мер защиты.

Для реализации рассмотренных в I-м разделе общих принципов инженерно-технической защиты информации (надежности, непрерывности, целеустремленности, активности, гибкости, скрытности, экономичности, комплексности) в условиях изменения условий необходимо управление силами и средствами системы. Учитывая, что традиционно подсистемы физической защиты и защиты от утечки курируются разными ведомствами, а пользователь информации один, то подсистема управления должна согласовывать деятельность сил и средств этих подсистем.

Нормативные указания отображаются в инструкциях по обеспечению защиты информации. Но в инструкциях невозможно учесть все ситуации. Силы и средства системы должны обеспечить принятие рационального решения при возникновении нетиповых ситуаций в условиях дефицита времени.

Так как защита информации невозможна без контроля ее эффективности, то важнейшей задачей подсистемы управления является организация и проведение различных видов контроля мер по защите.

В соответствии с системным подходом подсистемы физической защиты информации и защиты ее от утечки при их автономном анализе рассматриваются как системы.

## 19.2. Подсистема физической защиты источников информации

Подсистема физической защиты информации создается для противодействия преднамеренным угрозам воздействия злоумышленника и стихийным силам, прежде всего пожару. Средства этой подсистемы реализуют методы физической защиты с помощью инженерных конструкций и технических средств охраны. Необходимость и эффективность инженерной защиты и технической охраны объектов подтверждается статистикой, в соответствии с которой более 50% вторжений совершается на коммерческие объекты со свободным доступом персонала и клиентов и только 5% — на объекты с усиленным режимом охраны, с применением специально обученного персонала и сложных технических систем охраны.

Основу средств инженерной защиты и технической охраны объектов составляют механические средства и инженерные сооружения, препятствующие физическому движению злоумышленника(ов) к месту нахождения объектов защиты, технические средства, информирующие сотрудников службы безопасности (охрану) о проникновения злоумышленника(ов) в контролируемую зону и позволяющие наблюдать обстановку в них, а также средства и люди, устраняющие угрозы.

Проникновение злоумышленников может быть скрытным, с механическим разрушением инженерных конструкций и средств охраны с помощью инструмента или взрыва, а в редких случаях в виде вооруженного нападения с нейтрализацией охранников. В соответствии с принципом многозональности и многорубежности защиты информации рубежи защиты создаются, прежде всего, на границах контролируемых (охраняемых) зон.

Состав подсистемы физической защиты может существенно отличаться: от деревянной двери с простым замком для большинства жилых квартир до автоматизированной системы охраны с группой быстрого реагирования крупной организации (предприятия). В общем случае структура подсистемы физической защиты представлена на рис. 19.2.


*Рис. 19.2.* Структура подсистемы физической защиты

Современную подсистему физической защиты организации (предприятия, фирмы) по решаемым задачам можно разделить на комплекс инженерной защиты источников информации и комплекс технической охраны.

Инженерную защиту информации обеспечивают:

естественные и искусственные преграды (барьеры) на возможном пути движения злоумышленников и распространения стихийных сил к источникам информации (или другим ценностям);

- преграждающие устройства систем контроля и управления допуском.

К **естественным преградам** относятся труднопроходимые участки местности, примыкающие или находящиеся на территории организации (рвы, овраги, скалы, речки, густые лес и кустарник), которые целесообразно использовать для укрепленности рубежей.

**Искусственные преграды** создаются людьми и существенно отличаются по конструкции и стойкости к воздействию злоумыш-

ленника. Ими являются заборы, стены, межэтажные перекрытия (полы, потолки), окна зданий и помещений. т. е. инженерно-архитектурные конструкции, являющиеся преградой на пути движения злоумышленника. Наиболее труднопреодолимые преграды для злоумышленника создают капитальные (бетонные и кирпичные) высокие (выше роста человека) заборы, стены и межэтажные перекрытия зданий.

Наименее стойкими преградами являются **двери** и **окна** зданий (помещений), особенно на первом и последнем этажах зданий и в местах близкого расположения окон от заборов, строений, наружных лестниц и деревьев. Из статистики квартирных краж, которая отражает слабые места инженерной защиты помещений, следует, что большинство краж совершается путем выбивания дверей, срыва петель, подбора ключей, проникновения через окна, форточки и балконы.

Окна укрепляют применением специальных, устойчивых к механическим ударам стекол и установлением в оконных проемах металлических решеток.

Двери и ворота — традиционные конструкции для пропуска людей или транспорта на территорию организацию или в помещение. Прочность дверей определяется толщиной, видом материала и конструкцией дверного полотна и дверной рамы, а также прочностью крепления и крепления рамы к стене и надежностью замков. Требования к прочности дверей указаны в ГОСТ Р 51072-97.

Последние рубежи защиты создают металлические шкафы, сейфы и хранилища. Поэтому к их механической прочности предъявляются повышенные требования. Металлические шкафы предназначены для хранения документов с невысоким грифом конфиденциальности, ценных вещей, небольшой суммы денег. Надежность шкафов определяется только прочностью металла и секретностью замков.

Для хранения особо ценных документов, вещей, больших сумм денег применяются **сейфы** и **хранилища**. К сейфам и хранилищам относятся двустенные металлические шкафы с тяжелыми наполнителями пространства между стенками, в качестве которых используются армированные бетонные составы, композиты, многослойные заполнители из различных материалов.

Традиционно для прохода людей и проезда транспорта на территорию организации используются калитки в заборе, двери здания и ворота для автотранспорта, закрываемые на замок. Для обеспечения санкционированного допуска людей и транспорта в контролируемые зоны создается **система контроля и управления доступом (СКУД) людей и транспорта**. Структурная схема контрольно-пропускного пункта (КПП) СКУД приведена на рис. 19.3.

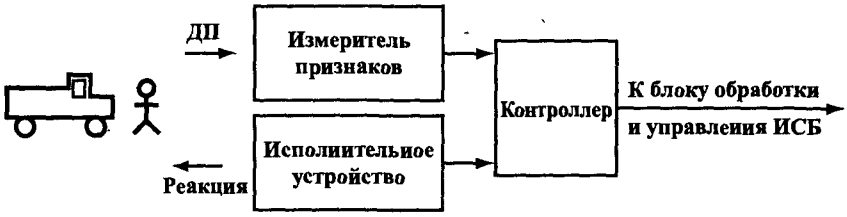



*Рис. 19.3.* Структура системы контроля и управления доступом

*Обозначения*: ДП — демаскирующие признаки, ИСБ — интегральная система безопасности.

Для обнаружения человека или автомашины необходимо измерить их демаскирующие признаки, используемые для идентификации, образовать текущие признаковые структуры, сравнить их с эталонными и по результатам сравнения принять решение о допуске или запрете на допуск объекта. Процедура идентификации (сравнения текущей признаковой структуры с эталонной) производится в контроллере (устройстве идентификации). Контроллер может использоваться в автономном режиме или в составе локальной сети интегральной системы безопасности. Пропуск объекта в контролируемую зону или его недопущение осуществляет исполнительное устройство.

Очевидно, чем более информативные признаки используются для идентификации, тем меньшие значения ошибок. Если допускается объект, не имеющий на это право, то возникает с вероятностью $P_{лд}$ ошибка ложного допуска (ошибка 1-го рода), если не допускается объект, имеющий допуск, то с вероятностью $P_{лз}$ возникает ошибка ложного запрета на допуск или ошибка 2-го рода. С точки зрения информационной безопасности, вероятность ложного допуска в большей степени характеризует надежность СКУД,

чем запрета на допуск. Вероятность ошибки 2-го рода уменьшает пропускную способность СКУД, которая оценивается количеством идентифицируемых объектов в единицу времени. В конечном счете, все объекты, имеющие допуск, после дополнительной процедуры идентификации будут допущены в соответствующую контролируемую зону. Пропущенные же злоумышленники могут причинить информации и не только ей непоправимый вред. Поэтому для обеспечения требуемого уровня безопасности информации от угроз преднамеренного воздействия вероятность ложного допуска должна быть не более допустимой, а вероятность ложного запрета — минимально возможной.

Ошибки допуска определяются, прежде всего, информативностью текущей и эталонной признаковых структур идентификаторов. Идентификатор представляет собой носитель демаскирующих признаков, которые используются для идентификации и принадлежат субъекту или объекту идентификации, имеющему допуск.

Для идентификации применяются **атрибутные** и **биометрические идентификаторы**. В качестве атрибутных идентификаторов используются автономные носители признаков субъекта или объекта. Например, ключ, открывающий дверь или ворота, разрешает вход человеку или въезд водителю, которые владеют ключом на момент допуска. В качестве атрибутных идентификаторов применяются также: спецодежда (форма работника МВД, халат врача или сестры), документ, удостоверяющий личность, или технический паспорт автомобиля, пропуск, идентификационные карточки, в которых именные признаки записываются на магнитной полосе, в штрих-коде, в структуре переизлучающего картой «Виганда» внешнего магнитного поля, в кодовой последовательности радиосигнала, излучаемого «проксимити» картой.

Ошибки идентификации возникают в случае ошибочной идентификации и если идентификатор с признаками одного объекта (субъекта) попадает к другому субъекту (объекту). Уменьшение ошибок идентификации человека или автотранспорта достигается:

- повышением информативности и количества демаскирующих признаков идентификаторов;
- надежной привязкой идентификаторов к объекту идентификации.

Ложный допуск объекта идентификации в контролируемую зону возникает не только за счет ошибок устройств идентификации, но и в результате подделки идентификаторов. Одна из оборотных сторон технического прогресса — проблема защиты атрибутных идентификаторов от подделки. Современные идентификационные карточки (штриховые, магнитные, «Виганда», Proximty) обеспечивают крайне малые ошибки идентификации. Некоторые из них (карты «Виганда» и «Проксимити») очень сложно подделать. Однако идентификационные карты слабо привязаны к объекту идентификации. Их могут похитить, купить и отобрать. В этом отношении даже самые защищенные карты не отличаются от идентификаторов времен гражданской войны — мандатов. Мандаты представляли собой лист бумаги, на котором были напечатаны или даже написаны от руки реквизиты (фамилия, имя, отчество представителя власти, занимаемая должность или выполняемые функции) и заверенные подписью выдавшего мандат лица и печатью учреждения. Единственным доказательством принадлежности мандата (так же как и бесконтактной «проксимити» карты) конкретному человеку являлось наличие мандата или карты у этого человека.

Для привязки атрибутного идентификатора к субъекту (объекту) принимаются различные меры вплоть до правовых. Например, к ответственности привлекаются люди, присвоившие не принадлежащий им атрибут, — надевшие для выполнения противозаконных действий форму военнослужащего или сотрудника правоохранительных органов. Наиболее часто для привязки идентификатора к конкретному человеку в идентификатор вносятся признаки этого человека. До изобретения фотографии признаки (приметы) человека (рост, характер телосложения, тип лица, форма носа, цвет глаз и волос и другие приметы) словами вписывались в атрибутный идентификатор, сейчас используется фотография его лица. Фотография лица — наиболее распространенное средство привязки идентификатора к конкретному человеку. Но фотографию можно заменить или даже изменить лицо с помощью пластической операции, что довольно часто наблюдается в уголовном мире.

Радикальным решением проблемы исключения подделки и кражи атрибутных идентификаторов является применение био-

метрических идентификаторов. В качестве биометрических идентификаторов используются именные признаки человека, потерять которые можно только вместе с соответствующим органом — носителем признаков, передать нельзя, а подделывают их в основном в боевиках. Наряду с традиционными отпечатками пальцев используются физиологические и динамические характеристики человека и его отдельных органов: рисунки радужной оболочки глаз и кровеносных сосудов на его сетчатке, термография (тепловое изображение лица), геометрия кисти, динамика подписи или печати на клавиатуре, спектральные характеристики речи человека. Значения показателей биометрических идентификаторов существенно различаются. Рисунки папиллярных линий пальцев, радужной оболочки и кровеносных сосудов сетчатки глаза обеспечивают вероятности несанкционированного пропуска, близкие к 0, но реализуются дорогостоящей аппаратурой. При использовании иных признаков ошибки выше, но средства дешевле. Кроме того, население пока психологически не готово к широкому внедрению этих средств СКУД. Например, рисунок радужной оболочки глаз содержит конфиденциальную информацию о состоянии здоровья человека которую использует медицина для диагностики его здоровья и которая, в случае использования для СКУД, может стать известна посторонним людям. Но сложность, цена радиоэлектронных средств и психологическая готовность пользователей к их применению — меняющиеся факторы, а достоинства биометрических идентификаторов очевидные и постоянные.

В простейшем варианте идентификацию людей по атрибутным идентификаторам производит на КПП охранник, который нажатием педали разблокирует вращающийся турникет для прохода допущенного человека. Такая организация пропускного режима, применяемая еще во многих госучреждениях и на промышленных предприятиях, имеет малую пропускную способность и низкую достоверность селекции, особенно в условиях дефицита времени. Когда перед глазами сотрудника охраны непрерывно проходит поток спешащих на работу людей, то в условиях психологического давления очереди резко возрастает вероятность ошибочной идентификации человека по фотографии на пропуске.

При применении идентификационных карточек и биометрических идентификаторов эту процедуру выполняют автоматы, ко-

торые производят считывание демаскирующих признаков с карточки или с человека, сравнивают их с эталонными, предварительно занесенными в память устройства, и по результатам сравнения выдают сигнал управления исполнительному устройству. Для считывания информации магнитные карты или карты со штрих-кодом проводятся через предусмотренную в считывающем устройстве прорезь или вставляются в соответствующую щель, что требует от идентифицируемого объекта внимательности и аккуратности. Более удобны идентификационные карты с возможностью дистанционного считывания признаков — карты Виганда и «Proximity». Для считывания признаков человека он должен предварительно ввести с пульта свой идентификационный номер, а затем приложить палец или кисть руки к окошку оптического считывающего устройства, направить взор на телевизионную камеру, написать определенное слово, ввести его с клавиатуры или произнести вслух. Считываемые данные преобразуются процессором компьютера или микропроцессором специального устройства идентификации в текущую признаковую структуру, которая сравнивается с эталонной, вызванной из базы эталонов предварительно вводимым идентификационным номером.

Физический допуск человека или автотранспорта в контролируемую зону осуществляет **исполнительное устройство (управляемое преграждающее устройство)**. Простейшим устройством является дверь. Если идентификатор — ключ не соответствует эталону в замке, дверь не открывается и запрещает проход в помещение. В организациях и общественных местах (на транспорте, стадионах и др.) широко применяются **вращающиеся двери, раздвижные и вращающиеся трех- или четырехштанговые турникеты** высотой до пояса и в полный рост. Турникеты имеют механизм блокирования вращения, который при разрешении допуска разблокируется педалью контролера (вахтера, охранника) или автоматически по сигналу управления. Наиболее совершенными исполнительными устройствами СКУД людей являются шлюзовые тамбуры, представляющие кабину с двумя дверьми. При проходе человека в шлюз входная дверь закрывается, а после прохождения процедуры идентификации по разрешающей команде контролера (вахтера) или автоматического устройства идентификации открывается выходная дверь. При отказе в допуске шлюзовой там-

бур позволяет задержать находящегося в нем человека для выяснения личности. Предусмотрен также режим аварийного выхода людей в случае неисправности исполнительного устройства или обесточивания СКУД. Для наблюдения за находящимся в тамбуре человеком его стены выполнены из ударопрочного стекла (бронестекла) или пластика. Внутри шлюза устанавливаются устройства определения атрибутных или биометрические идентификационных признаков, а также могут быть установлены детекторы металлических предметов для обнаружения оружия или радиоэлектронных средств, не разрешенных для проноса на контролируемую территорию, а также телевизионная камера наблюдения.

Контрольно-пропускной пункт на входе организации включает:

- зал со средствами контроля и управления доступом для прохода людей;
- бюро пропусков;
- камеру хранения вещей персонала и посетителей, не разрешенных для проноса в организацию;
- помещения для начальника охраны, дежурного контролера, размещения охранной сигнализации и связи и другие;
- средства контроля и управления доступом транспорта.

Конструкция, состав и количество КПП определяются размерами территории организации и количеством персонала. КПП должны обеспечивать необходимую пропускную способность людей и транспорта. Запасные входы и проезды для пропуска людей и транспорта в аварийной ситуации в нормальных условиях закрываются, пломбируются или опечатываются.

**Подкомплекс обнаружения** должен оповещать сотрудников службы безопасности, прежде всего охранников, органы вневедомственной охраны, милицию, пожарную охрану о проникновении злоумышленников на охраняемую территорию, о пожаре или иных стихийных бедствиях, защита от которых предусмотрена задачами системы.

Для обнаружения попыток преодоления злоумышленником барьеров и механических преград, а также пожара применяются **технические средства охраны объектов (ТСО)**, построенные на различных физических принципах.

Совокупность ТСО, предназначенных для решения **определенной группы** задач обнаружения источников преднамеренных угроз, образует подкомплекс ТСО, представляющий собой вариант подкомплекса обнаружения источников угроз (рис. 19.2). Структура типового подкомплекса ТСО автономного комплекса охраны представлена на рис. 19.4.

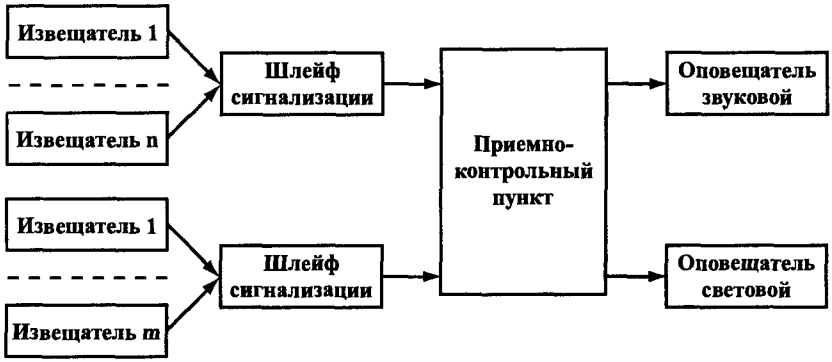



*Рис. 19.4.* Структура подкомплекса ТСО

**Извещатель** (датчик) охранный (охранно-пожарный, пожарный) представляет собой техническое устройство, формирующее электрический сигнал тревоги при воздействии на него механических сил и полей от злоумышленника и пожара. Так как обнаружить злоумышленника и пожар можно по их демаскирующим признакам, то извещатель предназначен для обнаружения этих демаскирующих признаках и формирования в случае их обнаружения сигнала тревоги, оповещающего об угрозах или управляющего в автоматическом режиме средствами нейтрализации угроз. Так как создать эффективные универсальные датчики или извещатели нельзя, то разработано большое количество типов извещателей, реагирующих на отдельные признаки злоумышленника и пожара или их комбинации. По назначению извещатели делятся на извещатели для блокирования отдельных объектов охраны, закрытых помещений, открытых пространств, периметров и обнаружения пожара. В зависимости от зоны обнаружения извещатели делятся на **точечные**, **линейные**, **поверхностные** и **объемные**. По виду признаков и способам их обнаружения извещатели делятся на **контактные**, **акустические**, **оптико-электронные**, **радиоволновые**, **вибраци-**

**онные, емкостные, тепловые, вибрационные и комбинированные**. Чем выше чувствительность извещателя, тем выше вероятность обнаружения злоумышленника и пожара, но одновременно выше вероятность ложной тревоги, соответствующей вероятности срабатывания извещателя от помех. Для уменьшения вероятности ошибки извещателя усложняют эталонную признаковую структуру. В акустических и радиоволновых извещателях для селекции сигналов, отраженных от движущегося злоумышленника, используется эффект Доплера. Сигнал тревоги в извещателе формируется лишь при превышении отклонения частоты отраженного сигнала от частоты излучаемого сигнала на величину не менее заданной, соответствующей частоте сигнала от движущегося злоумышленника. В оптическом диапазоне отклонения длин волн излучаемого и отраженного света столь малы, что измерить их достаточно просто не удается. Поэтому для селекции сигналов от злоумышленника от помех используются другие решения. Например, приемники пассивных оптико-электронных извещателей имеют многолучевую диаграмму направленности. Сигнал тревоги возникает, если инфракрасное излучение от злоумышленника последовательно принимается с разных направлений (лучей диаграммы направленности), что возможно, если злоумышленник движется перпендикулярно к направлению лучей.

Для снижения ошибок повышают количество используемых для принятия решения признаков, вводя их в память микропроцессора. Например, для обнаружения разбития стекла окна или витрины в качестве эталона используются спектральные и динамические характеристики сигналов, возникающих при его разрушении. Признаки акустических помех, в том числе образующиеся при ударе по стеклу без его разрушения, отличаются от эталонных признаков. В результате этого удается с большей вероятностью распознать акустические сигналы при разбитии стекла на фоне многочисленных акустических помех.

Значительное уменьшение ошибок обнаружения достигается в комбинированных извещателях за счет принятия решения в нем о вторжении злоумышленника по данным разных датчиков, например оптических и радиоволновых.

**Шлейф сигнализации** (охранной, пожарной, пожарно-охранной) образует электрическую цепь обеспечивающих электричес-

кую связь извещателей и приемно-контрольного прибора. В целях экономии соединительных проводов извещатели группируются, а шлейфы соединяют группу извещателей с приемно-контрольным прибором. Например, охранные и пожарные извещатели, установленные в одном помещении, передают в случае срабатывания сигналы тревоги по одному шлейфу. Извещатели, подключенные к одному шлейфу, должны иметь однотипные выходные цепи — с нормально замкнутыми или нормально разомкнутыми контактами. Эквивалентная схема шлейфа, соединяющего извещатели с нормально замкнутыми контактами, приведена на рис. 19.5.

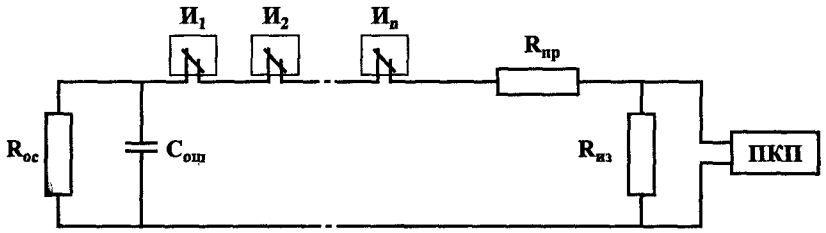



*Рис. 19.5.* Эквивалентная схема шлейфа

*Обозначения*: $И_n$ — n-й извещатель; ПКП — приемно-контрольный прибор; $R_{пр}$ — сопротивление проводов шлейфа; $R_{из}$ — сопротивление изоляции проводов шлейфа; $R_{ос}$ — согласующее сопротивление; $C_{ош}$ — электрическая емкость шлейфа.

Чем больше используется шлейфов, тем точнее локализованы места установки извещателей и тем точнее определяют силы нейтрализации угроз место вторжения их источников. Но при этом возрастают затраты на установку ТСО. Кроме того, целесообразно иметь разные шлейфы охранной и пожарной сигнализации. В этом случае можно обеспечить круглосуточную пожарную охрану, а средства охранной сигнализации в рабочее время отключать.

**Приемно-контрольные приборы (ПКП)** предназначены для приема и обработки сигналов, поступающих от извещателей, оповещения звуковым и световым сигналом сотрудников охраны о поступлении сигналов тревоги, нарушениях работы извещателей и шлейфов.

Все шире применяемые телевизионные средства наблюдения составляют основу **подкомплекса наблюдения (подкомплекса охранного телевидения)**. В него входят также средства дежурного

освещения, обеспечивающие необходимый уровень освещенности охраняемой территории в ночное время. Подкомплекс наблюдения обеспечивает возможность визуального дистанционного контроля за охраняемой территорией и действиями злоумышленников и, что важно для последующего криминалистического расследования, запись изображений произошедших чрезвычайных событий. Кроме того, возможности современных средств наблюдения позволяют автоматически обнаруживать проникновение злоумышленника в контролируемые зоны и решать задачи охраны, конкурируя в некоторых случаях со средствами подкомплекса обнаружения. В связи с существенно расширенными возможностями средств телевизионного наблюдения они в настоящее время рассматриваются как средства охранного телевидения.

Основной задачей **подкомплекса нейтрализации** является прекращение проникновения злоумышленника или стихийных сил к источнику путем воздействия на них. Типовая подсистема нейтрализации угроз имеет в своем составе силы и средства для физического и психологического воздействия на злоумышленников, проникших на охраняемую территорию, а также средства тушения пожара. Так как комплекс охраны становится неработоспособным при выключении электропитания, то одними из основных средств подкомплекса нейтрализации являются средства аварийного и резервного электропитания, источники которого автоматически подключаются вместо основного сетевого. Нейтрализация угроз является необходимой функцией любого комплекса охраны, так как при ее отсутствии невозможно в принципе обеспечить безопасность источников информации, как и любых других объектов защиты. Возможности нейтрализации угроз определяют время реакции подсистемы физической защиты информации.

Основной силой подкомплекса нейтрализации является человек — охранник. Он может состоять в штате подразделения охраны организации или быть сотрудником государственной или частной охранной структуры. Меньшее время реакции сил нейтрализации угроз обеспечивается, когда организация сама себя охраняет. В этом случае дежурная смена или сил быстрого реагирования размещается на территории организации, недалеко от мест проникновения. Кроме того, при периодическом обходе территории охран-

ники могут заметить вторжение или начало пожара до срабатывания технических средств и оперативно разобраться в обстановке. В некоторых организациях в ночное время для охраны привлекаются также сторожевые собаки, превосходящие по чувствительности и надежности лучшие образцы средств охраны.

Но эксплуатация **комплеска автономной охраны** требует больших расходов. Действительно, для обеспечения круглосуточной охраны минимальный штат сотрудников подразделения охраны составляет 7 человек: по 2 человека в каждой из 3 смен плюс один человек для замены больных и отпускников. Заработная плата охранников в течение нескольких лет может превысить разовые затраты на технические средства охраны. Бюджет далеко не многих, даже достаточно крупных коммерческих структур в состоянии выдержать такую финансовую нагрузку. Поэтому все более широко применяются комплексы **централизованной охраны**, в которых силы нейтрализации злоумышленников являются общими для нескольких организаций. Структурная схема комплекса централизованной охраны показана на рис. 19.6.

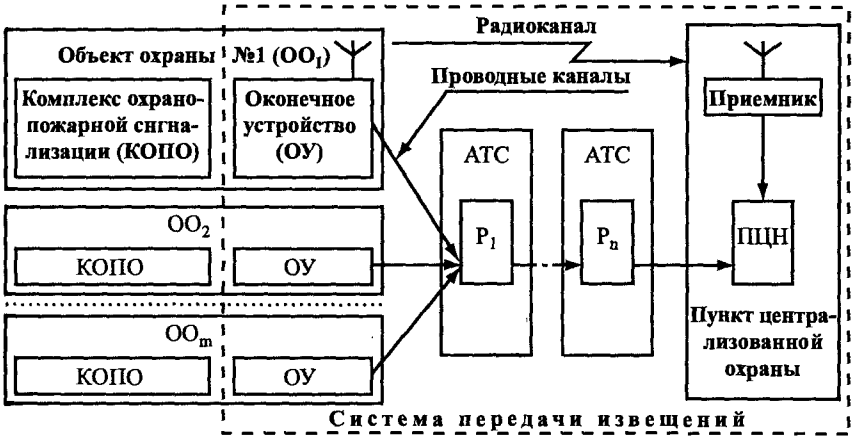



*Рис. 19.6.* Комплекс централизованной охраны

*Обозначения*: Р — ретранслятор; ПЦН — пульт централизованного наблюдения.

Примером охраны централизованного комплекса является охрана отделений филиалов сберегательного банка, мелких фирм, час-

тных домов, дач, квартир. Некоторые рядом территориально расположенные фирмы, например в одном здании, могут иметь общее подразделение охраны. Эффективную централизованную охрану обеспечивают подразделения вневедомственной охраны МВД.

В комплексах централизованной охраны извещения (сигналы проверки работоспособности комплексов охранно-пожарной сигнализации и тревоги от них) передаются после взятия объекта под охрану по проводным или радиоканалам на пульт централизованного наблюдения пункта централизованной охраны, который информирует оператора световым и звуковым сигналами о неисправности и тревоге. В качестве проводных линий связи для передачи извещений в большинстве случаях используются линии телефонов, установленных на объекте охраны. В простых случаях на время охраны телефонные линии подключаются к средствам охраны. Для обеспечения совместной телефонной связи и передачи извещений на концах телефонной линии устанавливается аппаратура уплотнения, например, частотного, которая обеспечивает передачу извещений без помех телефонной связи. При отсутствии телефонной связи извещения передаются по радиоканалу с помощью передатчика в УКВ диапазоне на объекте охраны и приемника на пункте централизованной охраны.

После поступления сигнала тревоги по команде оператора на объект охраны выезжает вооруженная группа сотрудников. Несмотря на довольно жесткие требования по времени (5–7 минут) прибытия группы охраны время реакции системы централизованной охраны больше, чем автономной, особенно если охраняемый объект находится далеко от места нахождения машины мобильной группы охраны. Кроме того, это время может быть в ряде случаев недопустимо увеличено в результате нарушения радиосвязи, «пробок» и ремонта на дорогах или путем, например, случайного или созданного дорожно-транспортного происшествия с машиной охраны, следовавшей к объекту, Но централизованные комплексы имеют большие возможности по нейтрализации угроз, особенно в виде вооруженного нападения.

Нейтрализация действий злоумышленников и пожара в комплексах охраны осуществляется сотрудниками службы безопаснос-

ти и средствами, функционально объединяемыми в подкомплекс нейтрализации угроз. Он может содержать:

- подразделение охраны автономного или централизованного комплекса;
- тревожную звуковую и световую сигнализацию;
- штатного или внештатного пожарника;
- средства пожаротушения;
- источники резервного (аварийного) электропитания.

**Подразделение охраны**, включающее в наиболее крупных и богатых организациях группу быстрого реагирования, составляет основу подкомплекса нейтрализации угроз. В автономном комплексе охраны подразделение охраны является элементом структуры организации, в централизованной используется подразделение охраны, общее для нескольких организаций, или подразделение вневедомственной охраны.

**Тревожная сигнализация** предназначена для психологического воздействия на скрытно проникающего в охраняемые зоны организации нарушителя с целью заставить его отказаться от намерения.

До недавнего времени для ликвидации пожара в любой организации в легко доступных местах размещались традиционные **средства пожаротушения**: пенообразующие огнетушители, механические средства (багры, топоры) для разрушения очага пожара, бочка с песком, пожарные рукава и др.

В конце XX в. произошли серьезные, качественные изменения в средствах пожаротушения, для которых характерны:

- вытеснение трудоемких в эксплуатации и ненадежных кислотных пенных огнетушителей более надежными и долговечными;
- автоматизация процессов пожаротушения.

Для тушения горючей среды разных классов применяют огнетушащие вещества: воду, пену, газ, порошок, аэрозоли и их комбинации. Однако не все указанные огнетушащие вещества пригодны для эффективного тушения разных горючих веществ. Некоторые сочетания горючего и огнетушащего веществ не только малоэффективны, но и могут ухудшить ситуацию. Например, при туше-

нии пожара водой, вызванного коротким замыканием электрических проводов, могут возникнуть новые очаги возгорания.

Источники **резервного (аварийного) электропитания** обеспечивают работоспособность основного элемента системы защиты информации при выключении основного источника электропитания.

## 19.3. Подсистема инженерно-технической защиты информации от ее утечки

Подсистема инженерно-технической защиты информации от утечки предназначена для снижения до допустимых значений величины риска (вероятности) несанкционированного распространения информации от ее источника, расположенного внутри контролируемой зоны, к злоумышленнику. Для достижения этой цели система должна иметь механизмы (силы и средства) обнаружения и нейтрализации угроз подслушивания, наблюдения, перехвата и утечки информации по вещественному каналу.

В соответствии с рассмотренной во втором разделе классификацией методов инженерно-технической защиты информации основу функционирования системы инженерно-технической защиты информации от утечки составляют методы пространственного, временного, структурного и энергетического скрытия.

Для обеспечения пространственного скрытия система должна иметь скрытые места размещения источников информации, известные только людям, непосредственно с ней работающим. В помещения, в которых хранятся секретные документы, имеет допуск очень ограниченный круг лиц. Руководители частных структур часто используют для хранения особо ценных документов тайники в виде вделанного в стенку и прикрытого картиной сейфа и даже отдельного помещения с замаскированной дверью.

Для реализации временного скрытия система защиты должна иметь механизм определения времени возникновения угрозы. В общем случае это время можно спрогнозировать, но с большой

ошибкой. Но в отдельных случаях оно определяется с достаточной точностью. К таким случаям относится время:

- пролета над объектом защиты разведывательного космического аппарата;
- работы радиоэлектронного средства или электрического прибора как источника опасных сигналов;
- нахождения в выделенном помещении посетителя.

Возможность точного определения места нахождения в космическом пространстве разведывательного космического аппарата (КА) позволяет организовать эффективную временную скрытность объекту защиты. Это время рассчитывается по параметрам орбиты запущенного КА специальной службой, которая информирует заинтересованные организации о расписании его пролета. Включение не прошедшего специальную проверку радиоэлектронного средства и электрического прибора создает потенциальную угрозу речевой информации в помещении, в котором установлено это средство или прибор. Поэтому разговоры по закрытым вопросам при включенных непроверенных или незащищенных радиоэлектронных средствах и приборах запрещаются. Также приход посетителя в выделенное помещение следует рассматривать как возникновение угрозы утечки информации. Поэтому в его присутствии исключаются разговоры и показ средств и материалов, не относящихся к тематике решаемых с посетителем вопросов. С целью исключения утечки информации через посетителей переговоры с ними за исключением случаев, когда в обсуждения возникает необходимость в демонстрации работы средств, проводятся в специальном выделенном помещении для переговоров, находящимся на минимальном расстоянии от КПП.

Средства структурного и энергетического скрытия существенно различаются в зависимости от угроз. Поэтому в общем случае подсистему инженерно-технической защиты от утечки информации целесообразно разделить на комплексы, каждый из которых объединяет силы и средства предотвращения одной из угроз утечки информации (рис. 19.7).


*Рис. 19.7.* Структура подсистемы защиты информации от утечки

**Комплекс защиты информации от наблюдения** должен обеспечивать:

- маскировку объектов наблюдения в видимом, инфракрасном и радиодиапазонах электромагнитных волн, а также объектов гидроакустического наблюдения;
- формирование и «внедрение» ложной информации об объектах наблюдения;
- уменьшение в случае необходимости прозрачности воздушной и водной среды;
- ослепление и засветку средств наблюдения в оптическом диапазоне длин волн;
- создание помех средствам гидроакустического и радиолокационного наблюдения.

Средства маскировки должны изменять видовые демаскирующие признаки поверхности защищаемого объекта под признаки

других объектов фона или признаков фона под признаки защищаемого объекта. Так как характеристики объектов наблюдения существенно различаются в акустическом, оптическом и радиодиапазонах, то средства маскировки в этих диапазонах также различаются.

Изменить структуру изображения объекта или фона можно и активными средствами — генераторами помех. Активные средства создают помеху, которая в зависимости от расположения генератора помех может создавать ложную точку или их совокупность на изображении объекта или фона. Путем размещения источников помех на поверхности объекта защиты или между простыми объектами сложного объекта изменяется его структура.

С помощью средств, изменяющих статические и динамические признаки объекта под признаки ложного объекта (объекта прикрытия), обеспечивается дезинформирование органов разведки.

**Комплекс защиты информации от подслушивания** включает средства, предотвращающие утечку акустической информации в простом акустическом канале утечки информации. Так как структурное скрытие речевой информации возможно в исключительных случаях (кодирование речевых сигналов), то основу средств рассматриваемого комплекса составляют средства энергетического скрытия. Они должны обеспечить:

- звукоизоляцию и звукопоглощение речевой информации в помещениях;
- звукоизоляцию акустических сигналов работающих механизмов, по признакам которых можно выявить сведения, содержащие государственную или коммерческую тайну;
- акустическое зашумление помещения, в котором ведутся разговоры по закрытой тематике.

Учитывая, что основу защиты информации от подслушивания составляют энергетические методы скрытия, то средства защиты от подслушивания должны, прежде всего, обеспечивать звукоизоляцию защищаемых акустических сигналов в контролируемой зоне. Звукоизоляция достигается созданием вокруг источника акустических сигналов ограждений и экранов, отражающих и поглощающих эти сигналы.

**Комплекс защиты информации от перехвата** должен предотвращать перехват защищаемой информации, содержащейся в ра-

дио- и электрических функциональных сигналах. С этой целью подсистема должна иметь средства, обеспечивающие:

- структурное скрытие сигналов и содержащейся в них информации;
- подавление до допустимых значений уровней опасных сигналов, распространяющихся по направляющим линиям связи (кабелям, волноводам);
- экранирование электрических, магнитных и электромагнитных полей с защищаемой информацией;
- линейное и пространственное зашумление опасных радио- и электрических сигналов.

Так как носителями информации в вещественном канале утечки информации являются отходы производства в твердом, жидком и газообразном виде, то средства **комплекса защиты предотвращения утечки вещественных носителей** должны обеспечивать:

- уничтожение информации, содержащейся в выбрасываемых или подлежащих дальнейшей переработке отходах;
- уничтожение неиспользуемых вещественных носителей;
- захоронение в специальных могильниках вещественных носителей, которые не могут быть уничтожены.

## 19.4. Управление силами и средствами системы инженерно-технической защиты информации

Эффективность любой системы в значительной степени зависит от эффективности управления ее силами и средствами. Без управления она раньше или позже ухудшит свои показатели и потеряет работоспособность. Бытует мнение, что эффективность хорошо работающей организации не зависит от присутствия или отсутствия на рабочем месте ее руководителя. Это утверждение отчасти справедливо для стационарных условий. Однако при появлении нетиповых ситуаций без руководителя не обойтись. Поэтому управление необходимо, прежде всего, для адаптации системы к изменениям условий ее функционирования. Чем более организованной и управляемой является система, тем более продолжительное

время она может противостоять многочисленным угрозам. Самые страшные болезни — рак и СПИД — возникают из-за поломки механизмов управления — иммунной системы человека, которая обнаруживает и нейтрализует источники внешних и внутренних угроз. У человека постоянно мутируют клетки, но здоровая иммунная система обнаруживает и уничтожает изменившиеся клетки, а ослабленная их пропускает, и они начинают непрерывно делиться. Иммунная система ВИЧ-инфицированного человек не способна его защитить даже от инфекции, которую здоровый человек не замечает.

Органы управления любой системы на основе данных о состоянии элементов системы, а также внешних и внутренних сигналов формируют команды управления, которые через управляемые объекты (другие элементы системы) обеспечивают решение системой поставленных задач и достижение ее целей. Внешние и внутренние воздействия на элементы системы изменяют ее состояние, определяющее, например, уровень безопасности информации. Сигнал тревоги от извещателя, например, характеризует с определенной вероятностью появление реальной угрозы защищаемой информации, Однако команды управления по ее нейтрализации могут существенно отличаться в зависимости от ситуации.

Простейшие команды управления представляют собой отклики на воздействия. В физиологии они называются безусловными и условными рефлексами. Долгое время (почти до середины XX в.) считалось, что рефлексы определяют поведение животных. Однако механизм их поведения оказался гораздо сложнее. По современным взглядам его основу составляют безусловные (генетические) и условные (формируемые при жизни) модели внутренней и внешней среды, в соответствии с которыми формируются команды управления.

**Основу управления силами и средствами инженерно-технической защиты также составляет ее модель.** Она представляет собой совокупность документов и программ, обеспечивающих достижение заданных значений показателей эффективности системы защиты. Модель содержит руководящие и нормативно-методические документы вышестоящих органов и разрабатываемые в ор-

ганизации. Например, к таким документам относятся положение о подразделении (его структуре, правах и обязанностях сотрудников), непосредственно обеспечивающее защиту информации, руководство по защите информации в организации, инструкция дежурным и др.

Управление силами и средствами защиты информации достигается путем долгосрочного и кратковременного планирования инженерно-технической защиты информации, нормативного и оперативного управления силами и средствами, а также контролем действий людей и работоспособности технических средств. План защиты является одним из основных элементов модели защиты. В нем на основе результатов состояния защиты и прогнозируемых угроз определяются необходимые меры по совершенствованию инженерно-технической защиты информации, сроки и должностные лица, ответственные за их реализацию. Нормативное управление представляет собой постановку задач и контроль их выполнения в соответствии с планом защиты.

Однако даже в очень подробном плане невозможно учесть все ситуации, которые могут возникнуть в реальных условиях. Более того, как показывает практика управления, чрезмерная детализация плана далеко не всегда приводит к повышению эффективности работы системы, особенно в случаях, когда разработчики планов недостаточно учитывают возможные условия. Лучшие результаты достигаются путем оперативного (ситуационного) управления. При оперативном управлении решение по защите информации принимается для конкретных условий появления нештатной (нетиповой) реальной угрозы. При оперативном управлении исходные данные более точные, чем при нормативном, но возникает, как правило, дефицит времени на принятие решения по нейтрализации возникшей угрозы. Дефицит времени может вызвать у лиц, принимающих решение, например у дежурного в ночное время, стрессовое состояние и привести к грубым ошибкам.

Необходимым условием эффективного управления является контроль выполнения плана и команд управления. Из-за недостаточного внимания к мерам контроля часто проваливаются хорошие планы. Обилие планов при недостаточном контроле за их

выполнением является признаком бюрократии, для которой разработка разнообразных планов становится самоцелью.

В общем случае для эффективного управления силами и средствами системы инженерно-технической защиты информации необходимо обеспечить:

- прогноз угроз;
- данные о состоянии сил и средств системы;
- модели объектов защиты и угроз;
- данные о выявленных технических каналов утечки информации;
- решения о мерах нейтрализации угроз в случае появления сигналов тревоги и других сигналов, требующих реагирования (например, об обрыве шлейфа);
- реализацию решений в виде команд силам и средствам нейтрализации угроз;
- контроль за посетителями организации;
- контроль за эффективностью принятых мер защиты.

Так как управление силами и средствами инженерно-технической защиты включает разнообразные специфические процессы, для выполнения которых необходимы соответствующие программно-аппаратные средства и специалисты, то объективно система инженерно-технической защиты информации должна иметь комплекс управления. Схема управления в системе инженерно-технической защиты информации приведена на рис. 19.8.

Комплекс управления объединяет сотрудников и технические средства, которые выполняют следующие функции:

- прогнозирование возможных угроз защищаемой информации;
- планирование мер по обеспечению требуемого уровня безопасности информации и контролирование их выполнения;
- контролирование работоспособности средств защиты;
- сбор и анализ сигналов и данных об источниках угроз информации;
- формирование команд (сигналов) управления силам и средствам об отражении и ликвидации угроз;
- анализирование нарушения в функционировании системы и ее элементах, разработка мер по их предотвращению.

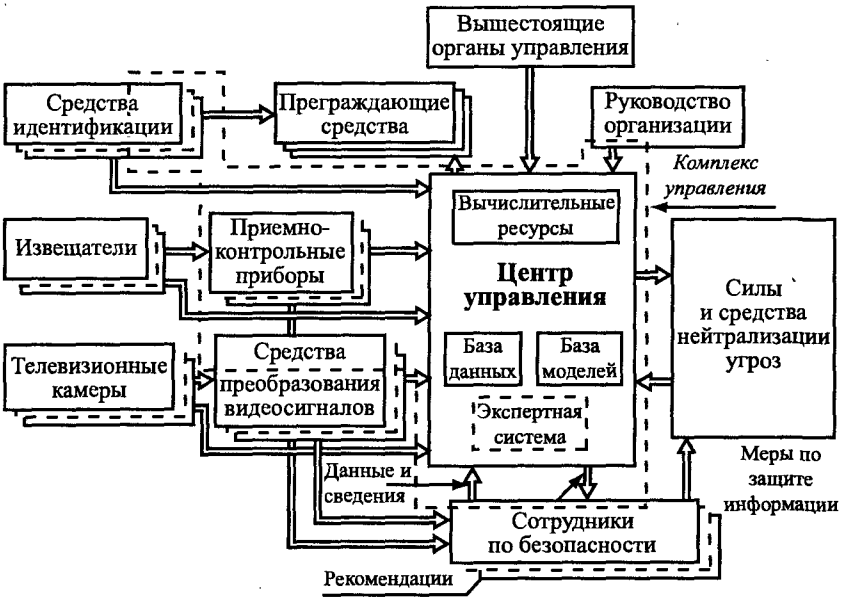



*Рис. 19.8.* Схема управления в системе инженерно-технической защиты информации

На рис. 19.8 силы и средства комплекса управления обведены пунктирной линией. Комплекс управления включает центр (пункт) управления, руководителей и сотрудников организации, участвующих в управлении, а также средства управления подсистем, комплексов и подкомплексов.

Источниками входных сигналов комплекса управления являются (рис. 19.8):

- вышестоящие органы управления и руководства организации;
- извещатели и приемно-контрольные приборы подкомплекса обнаружения источников угроз;
- телевизионные камеры и преобразователи видеосигналов, формирующие изображение для оператора и сигналы тревоги;
- средства идентификации людей и автотранспорта;
- сотрудники службы безопасности, выявляющие технические каналы утечки информации и разрабатывающие меры по их ликвидации.

Наличие в комплексе разнообразных средств локального управления обусловлено поэтапным развитием методов и средств управления. Можно выделить три этапа:

- автономное управления различными комплексами;
- объединение средств управления вокруг одного или нескольких компьютеров;
- централизация управления.

До появления мощных персональных компьютеров управление средствами осуществлялось сотрудниками по безопасности по сигналам средств управления доступом и технической охраны объектов.

В простейших СКУД управление допуском людей и автотранспорта на территорию организации осуществляет сотрудник охраны, который по результатам идентификации разблокирует (открывает) преграждающее устройство. В современных автономных СКУД команда преграждающему устройству по результатам идентификации формирует логическое устройство.

Управление работой (включение, выключение, контроль) извещателей, проверка целостности шлейфов автономных и централизованных систем технической охраны (подкомплекса обнаружения на рис. 19.2) производится с помощью приемно-контрольных приборов (ППК), к которым подключаются шлейфы от извещателей. В ППК формируются звуковые и световые сигналы, информирующие операторов о режимах работы, срабатывании извещателей и обрывах в шлейфах, по которым принимаются решения по отражению и ликвидации угроз.

В системе видеонаблюдения (на рис. 19.2 в подкомплексе видеоохраны) оператор управляет телевизионными камерами и осуществляет действия по нейтрализации угроз, обнаруженных по изображениям на мониторах или реагируя на сигналы тревоги детекторов движения. Автоматические включение телевизионной камеры по сигналу тревоги извещателя и видеозапись изображения в зоне нахождения этого извещателя существенно повысили обоснованность принятия решений.

Система охраны крупной организации и музея включает десятки и сотни извещателей, десятки телевизионных камер и дру-

гие элементы, от которых постоянно поступает информация. Ее надо обработать в реальном масштабе времени и принять по ней решение, что невозможно сделать вручную малочисленной дежурной смене охраны. С увеличением количества извещателей и телевизионных камер, устанавливаемых в организации, ужесточением требований к пропускной способности и вероятности ошибок СКУД возникла необходимость в автоматизации управленческих решений.

Основными задачами автоматизации являются следующие:

- повышение оперативности управления, влияющей на время реакции системы на вторжение;
- локализация места вторжения злоумышленника или возникновения пожара;
- непрерывный контроль работоспособности технических средств и сил охраны;
- обнаружение попыток злоумышленников нарушить работоспособность технических средств охраны.

Для автоматизации процессов управления используются вычислительные ресурсы и базы данных и моделей центра управления, сопрягаемые со средствами обнаружения, видеоконтроля, идентификации и нейтрализации угроз. В перспективе к ним добавиться экспертная система, помогающая дежурной смене принимать решения по защите информации на уровне специалистов высокой квалификации.

Совокупность средств, объединяемых средствами управления, составляет техническую основу **интегрированной системы охраны (ИСО)**. В зависимости от состава средств интегрированные системы охраны различают по уровням. Система первого уровня (ИСО-1) объединяет средства охранной, пожарной и охранно-пожарной сигнализации и средства СКУД на территорию организации. ИСО-2 дополняется средствами видеонаблюдения. В ИСО-3 используются полный набор технических средств, в том числе СКУД в отдельные зоны, управление которыми осуществляется с помощью компьютеров.

Интегрированные системы имеют иерархическую структуру и реализуются на базе адресных панелей, обслуживающих используемые датчики (охранные, охранно-пожарные, пожарные, извещатели, видеокамеры, считыватели электронных замков и др.) и ис-

полнительные устройства (оповещатели тревожной сигнализации, исполнительные механизмы замков, пиропатроны модулей газового пожаротушения и др.), а общее управление системой осуществляется одной или несколькими мощными ПЭВМ.

В адресной панели реализуется модульный принцип, что дает возможность регулировать состав оборудования в зависимости от сложности объекта. Эти панели включают в свой состав также источники резервного питания.

Состояние охраняемых объектов отображается в графическом виде на рабочем месте оператора. На экране монитора рисуется план выбранной территории с указанием состояния каждой отдельной зоны в сопровождении текста, звуковых и речевых сигналов (например, о тревожной ситуации). На экран в полиэкранном режиме могут выводиться изображения от соответствующих телекамер.

Средства комплекса управления регистрируют с указанием времени:

- «тревожные» события, возникающие в случае тревожных или нештатных ситуаций;
- «охранные» — о постановке и снятии с охраны зон охраняемых объектов;
- «действия оператора», определяемые как вмешательство в работу системы, так и реакции на тревожные события;
- «неисправности», вызванные выходом из строя аппаратуры, нарушением линий коммуникаций или несанкционированным вмешательством в работу системы.

Наличие мощного компьютера, разветвленной сети линий связи и автоматизированной системы контроля и управления допуском позволяют в рамках интегрированной системы безопасности решать дополнительные важные задачи, в том числе:

- автоматический учет рабочего времени персонала организации;
- учет присутствия персонала на рабочих местах;
- определение местонахождения сотрудников и посетителя на территории организации;
- дистанционный контроль за состоянием дверей, турникетов, шлагбаумов, ворот, датчиков охранно-пожарной сигнализации;

- оперативное изменение режимов работы организации или отдельных сотрудников;
- контроль за работой дежурной смены.

При установке на дверях служебных помещений средств контроля и управления доступом возникает возможность непрерывного определения местонахождения сотрудников и посетителей, учета времени нахождения сотрудника на рабочем месте (в рабочем помещении), накапливать данные о подозрительных передвижениях (интересе) отдельных сотрудников и др.

Длительное время не удавалось решить проблему контроля за работой сотрудников охраны в ночное время, у которых в условиях спокойной обстановки в течение длительного времени снижается психологическая установка на угрозу. В результате этого снижается внимательность во время наблюдения изображений на экранах мониторов, ухудшается пунктуальность выполнения требований инструкций, нарушается регулярность обхода территории и появляются другие нарушения, вплоть до сна на посту. Эта проблема возникает в любых организациях с ночными сменами. Она эффективно решается в интегральных системах безопасности путем периодической подачи в случайные моменты времени компьютером дополнительных сигналов. На эти сигналы охранник должен выполнить указанные в инструкции определенные действия, например нажать конкретную клавишу клавиатуры. При обходе территории охранник должен нажать установленные на маршруте кнопки. По времени нажатия клавиш и кнопок, величине отклонения относительно времени подачи контрольных сигналов оценивается качество работы охраны.

Повышение эффективности управления централизованными комплексами охраны обеспечивается автоматизацией процессов контроля и охраны (взятия под охрану и снятия с нее), обработка сигналов извещателей, регистрации состояния охраняемых объектов и принятых мер.

Дальнейшая интеграция предусматривает сопряжение ИСО с силами и средствами предотвращения утечки информации в рамках интегральной системы безопасности (ИСБ).

Основными элементами так называемых **систем передачи извещений (СПИ)** являются оконечные устройства (интерфейсы), устанавливаемые на охраняемых объектах, ретрансляторы, как

правило, на АТС и пульты на пунктах централизованной охраны. Для передачи извещений и команд управления используются линии телефонной связи, специальные проводные линии, радиоканалы, комбинированные линии связи.

## 19.5. Классификация средств инженерно-технической защиты информации

Средства инженерно-технической защиты информации реализуют рассмотренные методы защиты информации от всех известных угроз. Их классификация на рис. 19.9 соответствует классификации угроз. На первом уровне классификационной схемы все средства инженерно-технической защиты разделены на 2 группы: средства противодействия угрозам воздействия и средства противодействия утечке информации.

**Средства противодействия угрозам воздействия** обеспечивают физическую защиту источников информации и их техническую охрану. Средства физической защиты включают инженерные конструкции и средства контроля и управления доступом в контролируемую зону людей и транспорта.

Средства технической охраны обеспечивают:

- обнаружение носителей угроз воздействия;
- наблюдение в контролируемой зоне за источниками угроз воздействия;
- нейтрализацию угроз воздействия;
- управление средствами технической охраны.

Так как угрозу утечки информации по оптическому каналу создает скрытное наблюдение, по акустическому каналу — подслушивание, в радиоэлектронном канале — перехват сигналов, а в вещественном канале — неконтролируемые выброс и сброс отходов дело- и технического производства, то **средства противодействия утечке информации** включают:

- средства противодействия наблюдению;
- средства противодействия подслушиванию;
- средства противодействия перехвату;
- средства защиты информации от утечки по вещественному каналу.

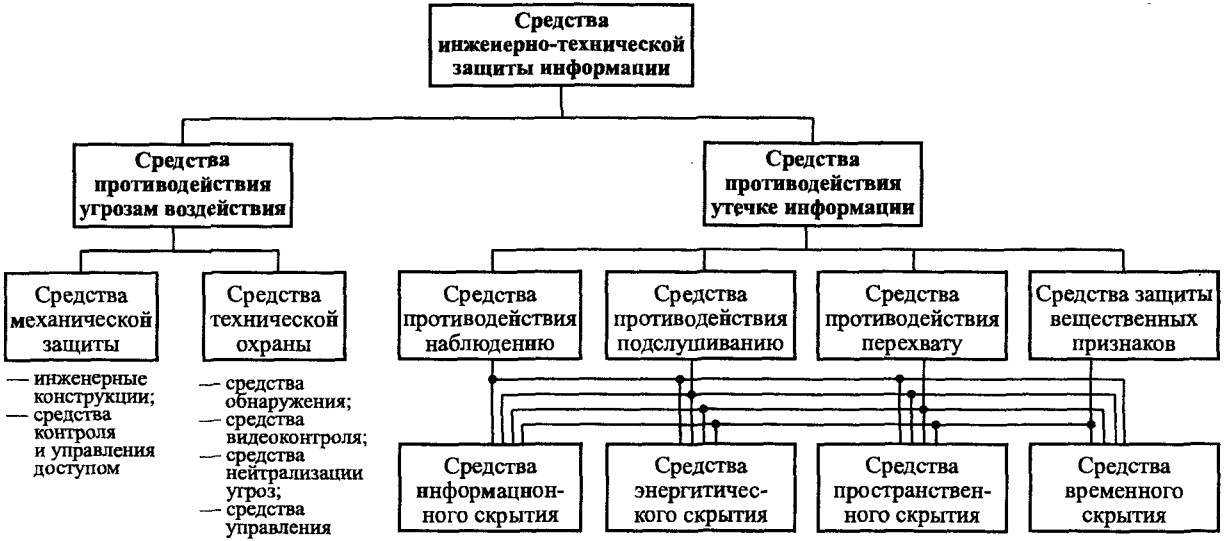



*Рис. 19.9.* Классификация средств инженерно-технической защиты информации

Предотвращение утечки информации в каждом из каналов обеспечивается одним из методов скрытия: временного, пространственного, структурного и энергетического скрытия. Следовательно, средства предотвращения утечки информации в любом из каналов утечки информации можно разделить на средства структурного, энергетического, пространственного и временного скрытия.

### Вопросы для самопроверки

1. Состав системы инженерно-технической защиты информации.
2. Основные функции комплексов подсистемы физической защиты источников информации.
3. Типы технических средств подсистемы физической защиты источников информации.
4. Назначение и состав средств системы контроля и управления доступом.
5. Типы идентификаторов. Преимущества и недостатки биометрических идентификаторов по сравнению с атрибутными.
6. Типы технических средств охраны.
7. Средства, применяемые для нейтрализации угроз.
8. Основные функции комплексов подсистемы защиты информации от утечки.
9. Типы технических средств подсистемы защиты информации от утечки.
10. Чем отличаются средства дистанционного и непосредственного подслушивания?
11. Влияние условий эксплуатации наземных технических средств добывания на их характеристики.

# Глава 20. Средства инженерной защиты

Средства инженерной защиты объединяют конструкции, затрудняющие движение злоумышленника и распространение стихийной силы к источнику информации, и включают ограждения территории, зданий и помещений, шкафы, сейфы и хранилища, а также средства системы контроля и управления доступом людей и транспорта в контролируемые зоны.

По степени защиты ограждения делят на 4 класса. Ограждения из различных некапитальных конструкций высотой не менее 2 м относятся к ограждениям 1-го класса. Деревянные сплошные ограждения толщиной не менее 40 мм, металлические сетчатые или решетчатые высотой не менее 2 м образуют ограждения 2-го класса. Железобетонные, каменные, кирпичные сплошные металлические ограждения высотой не менее 2,5 м представляют собой ограждения 3-го класса. Монолитные железобетонные, каменные, кирпичные ограждения высотой 2,5 м, оборудованные дополнительным ограждением, являются ограждениями 4-го класса.

## 20.1. Ограждения территории

Ограждения территории — наиболее древние инженерные конструкции для физической защиты объекта или его отдельных участков от проникновения злоумышленника на охраняемую территорию. По назначениям они делятся на **основные, дополнительные и предупредительные**. Дополнительные ограждения предназначены для повышения укрепленности основных ограждений. Предупредительные ограждения устанавливаются с внутренней или внешней стороны основного ограждения и предназначены для ограничения доступа к нему людей. На предупредительном ограждении устанавливаются запрещающие таблички типа «Запретная зона», «Не подходить», «Стой» и др.

Основным ограждением территории организации является забор. Заборы можно разделить на **декоративные** и **защитные**. Декоративные заборы обозначают на местности границу территории организации и создаются кустарником, столбиками, тросами, проволокой и др.

Защитные заборы препятствуют проникновению людей, автотранспорта и животных на территорию организации. Различают следующие основные типы защитных заборов:

- монолитные;
- сборные бетонные или железобетонные;
- металлические (литые, кованые, сварные);
- сетчатые;
- проволочные;
- деревянные;
- растительные (живая изгородь);
- комбинированные.

Монолитные железобетонные, каменные, кирпичные заборы изготовляются из строительных материалов на месте установки и представляют собой наиболее прочные конструкции. Они имеют высоту 1,8–2,5 м, мощный цоколь (фундамент) и стены толщиной порядка 30 см.

Сборные железобетонные заборы состоят из фундаментальных опор («башмаков») и вставляемых в них сплошных железобетонных плит или из вертикальных опор с пазами, в которые вставляются железобетонные секционные плиты. Высота стандартных плит около 2,5 м, расстояние между опорами составляет 2,5; 3; 4 м. Но железобетонные плиты сборных заборов тоньше монолитных и проламываются ломом.

Металлические заборы выполняются в виде литых ажурных конструкций или ограждений из прямоугольных и круглых окрашенных профилей. Металлические заборы обычно прозрачны для наблюдения, но иногда их закрывают с внутренней стороны металлическими листами. Металлические открытые заборы не создают серьезных преград для злоумышленников: их нетрудно перелезть, проделать лаз, раздвинув прутья домкратом, перерезать прутья, подлезть под забор. Используют такие ограды в основном в населенных пунктах, где повышенные требования по архитектурному оформлению объектов.

Для создания сетчатых заборов применяются сварная металлическая сетка и сетка свободного плетения (сетка «Рабица») высотой до 2,2 м. Сетчатый забор легко преодолевается сверху, в нем достаточно просто вырезать лаз кусачками. С целью уменьшения

помех извещателям, вызванных их колебаниями под действием ветра, применяют также более дорогие сварные сетчатые полотна. Как правило, сетчатые заборы используются на простых объектах в качестве основных ограждений, на важных объектах — как дополнительные ограждения.

Проволочные ограждения изготавливаются из колючей и гладкой проволоки. Ограждения из гладкой проволоки высотой порядка 1,5–1,8 м используются как дополнительные и предупредительные ограждения внутри объекта. Ограждения из колючей проволоки могут быть основными и вспомогательными. Основные ограждения могут быть многорядными или выполняться в виде спиралей. Такие ограждения используют для блокирования временных складских площадок, военных объектов или объектов специального назначения.

Наиболее слабую защиту имеют деревянные сплошные и разреженные заборы. Под действием ветровой нагрузки они создают вибрационные и импульсные механические помехи, увеличивающие вероятность ложного срабатывания установленных на них извещателей. Деревянное забор-ограждение из реек (штакетник) используется в основном как предупредительное дополнительное ограждение. Извещатели на них не устанавливаются.

Комбинированные заборы содержат участки различной конструкции. Прочность забора определяется прочностью наиболее слабого участка.

Для создания злоумышленнику дополнительных препятствий сверху кирпичных и бетонных заборов устанавливают дополнительные ограждения — проволочное ограждение («козырек») в три–четыре нитки, смонтированное на специальных кронштейнах, острые стержни или битое стекло. Для защиты верхней части капитальных заборов применяется также армированная колючая лента (АКЛ), изготавливаемая путем армирования колючей ленты стальной оцинкованной проволокой диаметром 2,5 мм. Колючая лента заградительная представляет собой оцинкованную ленту толщиной 0,5 мм, имеющую обоюдоострые симметрично расположенные шипы. Например, для наземных заграждений, козырьков над заборами и крышами выпускают спирали из АКЛ диаметром 500–

955 мм и длиной 10–20 м. Для предотвращения проникновения под забором его укрепляют нижним дополнительным ограждением в виде бетонированного или решетчатого цоколя, заглубляемого под основное ограждение на глубину 40–50 см.

Для размещения средств периметровой сигнализации, телевизионного наблюдения, связи, освещения, тропы движения сотрудников охраны и собак, а также постовых укрытий между основным и предупредительным заборами создается **зона отторжения**. Если в зоне отторжения устанавливаются технические средства охраны периметра, то ширина зоны отторжения устанавливается не менее ширины их зоны обнаружения. Для обнаружения прохода злоумышленника через зону отторжения она может оборудоваться контрольно-следственной полосой из взрыхленного грунта шириной не менее 1,5 м.

На отдельных участках ограждения с пониженной защищенностью в полосе отторжения могут размещаться ловушки в виде объемных проволочных сетей. Объемная сеть представляет собой проволочное плетение в виде пространственной четырехъярусной сети, выполненной из кольцевых гирлянд диаметром 0,5–0,6 м и соединенных между собой по длине и высоте отдельными скрутками из мягкой проволоки. Диаметр проволоки составляет 0,5–0,9 мм. Ноги перелезшего через забор злоумышленника застревают в проволочной сети, и ему крайне трудно выбраться из нее без посторонней помощи.

Под заборами для стока вод устанавливают водопропуски из железобетонных или металлических труб. На трубы диаметром более 30 см устанавливают металлические решетки.

Достоинством мощных ограждений является также психологическое воздействие их на, прежде всего, неподготовленного малоквалифицированного злоумышленника, под влиянием которого злоумышленник может отказаться от преступного замысла.

## 20.2. Ограждения зданий и помещений

К ограждениям зданий и помещений относятся двери, окна, стены зданий и помещений, полы и потолки. Наиболее слабыми ограждениями являются двери, ворота и окна.

### 20.2.1. Двери и ворота

Двери и ворота — традиционные конструкции для пропуска людей или транспорта на территорию организации или в помещение. В ГОСТ Р 50862 дверь защитная определяется как «устойчивое к взлому устройство, состоящее из дверной коробки с подвижно закрепленным на нем полотном, которое в закрытом положении фиксируется в дверной коробке замковым устройством или запирающим механизмом, соответствующее классу устойчивости к взлому, меньшему чем дверь хранилища ценностей». Двери с застеклением (балконные, в коридоре, в помещении) рассматриваются как окна.

Прочность дверей (в терминологии стандартов — управляемых преграждающих устройств — УПУ) характеризуется устойчивостью к взлому, пулестойкостью, устойчивостью к взрыву. Различают двери с нормальной, повышенной и высокой устойчивостью.

**Нормальную устойчивость** имеют двери, выдерживающие динамические нагрузки до 90 Дж. Двери **повышенной устойчивости** противостоят взлому одиночными ударами и/или с применением различных инструментов. Пулестойкие двери и двери, устойчивые к взрыву, относятся к дверям с **высокой устойчивостью**. По устойчивости к взлому двери делятся на классы.

Двери 1-го класса защищены от взлома приложением статических нагрузок, ударных нагрузок без и с применением ручного механического инструмента, а также от воздействия ручного рычажного или раздвигающего инструмента. Двери 2-го и 3-го классов должны выдерживать соответственно увеличенные и повышенные статические и ударные нагрузки. Двери 4-го класса должны обеспечивать защищенность от взлома с приложением высоких статических нагрузок, ударных нагрузок ручным механическим инструментом ударного действия и от воздействия силового ручного рычажного или раздвигающего инструмента, а также от воздействия электрического инструмента режущего и/или ударного действия. Классу 5 соответствуют двери, выдерживающие воздействие электрического инструмента режущего и/или ударного действия повышенной мощности, а также термического режущего инструмента и/или сварочного оборудования.

Обычные филенчатые двери и двери с так называемой «сотовой» структурой обеспечивают слабую защиту от взлома и относятся к дверям 1-го класса. Прочность дверей может быть повышена следующими способами:

- изменением направления открывания двери с «от себя» на «на себя», затрудняющего ее выдавливание и выбитие;
- изготовлением дверного полотна из цельных лесоматериалов крепких пород деревьев;
- установлением с обеих сторон дверного полотна стальных полос, стягиваемых болтами;
- обивкой дверных деревянных полотен металлическими листами;
- укреплением дверной коробки стальными уголками в местах крепления петель и запорных планок замков;
- «прибитием» дверной коробки к проему стены с помощью стальных штырей;
- установкой перед дверью, открываемой наружу, стальной планки, закрываемой дополнительным замком;
- установкой параллельно двери распашной или раздвижной стальной решетки, закрываемой дополнительным замком.

Для укрепления полотна двери используются стальные накладки толщиной 1,5–2,5 мм, установленные с обеих сторон. Более значительно усиливает конструкцию дверей обивка двери металлическим листом толщиной 1–3 мм или изготовление ее целиком из железа. Стальные двери представляют собой короб из двух листов стали, приваренных к выполненным из стального профиля ребрам жесткости и между которыми размещают звуко- и теплоизоляционную прокладку. Бронированные двери из высоколегированной специальной стали толщиной 6 мм с наполнителем из базальтовой ваты способны выдержать удар пули автомата Калашникова.

**Взломоустойчивость ворот** характеризуется 4 степенями защиты. Ворота 1-й степени защиты от взлома выполняются из некапитальных материалов и конструкций высотой более 1,5 м. Деревянные ворота высотой не менее 2 м и толщиной не менее 40 мм имеют 2-ю (среднюю) степень защиты. Третью (высокую) степень защиты имеют комбинированные или силовые ворота высотой не менее 2,5 м и классом устойчивости не ниже VI по

ГОСТ 51242-98. Металлические ворота высотой не менее 2,5 м с устойчивостью не менее С1 (согласно ГОСТ 51242-98) имеют 4-ю степень защиты.

Надежность дверей и ворот определяется не только их толщиной, механической прочностью материала и средств крепления к стене, но и надежностью замков. За свою историю люди придумали разнообразные замки. По способу открытия (закрытия) современные замки делятся на **механические** и **электроуправляемые**.

**Механические замки** открываются (закрываются) механическим ключом, а механические кодовые замки открываются путем механического воздействия на рычаг после набора на их пульте определенного набора цифр — кода.

Для всех механических замков характерно наличие **ригеля (засова), сувальд, ключа, корпуса** и **запорной планки**.

**Ригель** представляет часть замка, непосредственно запирающую дверь, ящик, крышку и т. п. Ригель состоит из головки, на которую действует ключ, и из одной или двух задвижек. Часть задвижки, входящая в отверстие планки, крепящейся на внутренней стороне дверной коробки напротив замка, называют языком замка. Замок с языком косой формы и подпружиненной задвижкой автоматически защелкивается при закрытии двери, вызывая иногда большую проблему у хозяина квартиры, описанную в романе Ильфа и Петрова «Двенадцать стульев». Для более надежного запирания дверей ригели делают из прочной стали, удлиненными и одновременно двигающимся в вертикальной и горизонтальной плоскостях. Роль засова в навесных замках выполняет его дужка.

Детали замка, которые толкают ригель под воздействием «своего» ключа, называются **сувальдами**. Конструкция и конфигурация подпружиненных сувальд образуют «секрет» ключа.

**Ключ** управляет механизмом замка, который бывает с индивидуальным или групповым (для определенной серии замков) секретом. Ключ ставит сувальды и пружины в такое положение, чтобы стало возможным передвижение ригеля. Каждый ключ делают такой формы, чтобы затруднить подделку. В далеком прошлом изготовляли ключи крупных размеров, которые носили на груди. Но чем больше отверстие для ключа, тем проще взлом замка. Поэтому сейчас стараются делать ключи минимально возможных размеров.

**Электроуправляемые замки** открываются и закрываются или только закрываютсяпри подаче на них электрического тока. К ним относятся электрические защелки, электромеханические, соленоидные, моторные и электромагнитные замки.

**Электрическая защелка** представляет собой механический защелкивающий замок, у которого устанавливаемая на дверной коробке пластина с отверстием для языка замка имеет откидную часть, управляемую электромагнитом. При поступлении в катушку электромагнита электрического тока планка не задерживает язык замка и дверь открывается без ключа. Достоинством электрической защелки является относительная дешевизна и малый потребляемый ток, составляющий сотни мА.

В **электромеханическом замке** электромагнит разблокирует поворотную ручку замка двери, которая для открывания двери поворачивается вручную. При этом дверь может быть открыта только в период действия управляющего сигнала. Конструктивно электромеханические замки могут быть накладные и врезные.

В **соленоидных замках** часть задвижки является одновременно сердечником соленоида (катушки с большим количеством провода, внутри которой может двигаться сердечник). В нормально закрытом замке при подаче электрического тока в катушку соленоида его сердечник втягивается вовнутрь катушки, язык выходит из отверстия запорной планки и дверь открывается. В другом варианте замка с помощью соленоида дверь закрывается. Существуют соленоидные замки с поворачиваемой щеколдой. Но соленоидные замки потребляют большой (до 5 А) ток.

В **моторных замках** ригель двигается с помощью электрического мотора. Они применяются в основном для открытия и закрытия ворот. Их недостатки — большие габариты и замедленное открывание в течение до 10 секунд.

Простой **электромагнитный замок** состоит из двух основных частей: электромагнита, укрепленного обычно на внутренней стороне верхней планки дверной коробки, и пластины, укрепляемой на торце дверного полотна напротив сердечника электромагнита. Когда в электромагнит подается электрический ток, то пластина им притягивается и удерживает дверь в закрытом состоянии. Усилие удержания зависит от величины щели между сердечником электромагнита и пластиной, магнитной проницаемости матери-

ала сердечника электромагнита и пластины и качества обработки их взаимных поверхностей. Хорошие магнитные замки обеспечивают усилие в 700 кг при токе 200–700 мА. Пластины более дорогих и редких магнитных замков имеют подвижную часть, которая притягивается находящимся под током электромагнитом и входит на несколько мм в углубление его сердечника. В результате этого к усилиям удержания электромагнита добавляется механическая прочность подвижной части пластины на сдвиг. Суммарные усилия достигают 1–2 тонн. Бесшумность работы, высокое быстродействие и большое усилие удержания магнитных замков обусловили их широкое распространение для управления доступом в подъезды жилых домов, оснащенных домофонами, и в служебные помещения организаций.

В зависимости от механизма обеспечения секретности различают **бессувальдные, сувальдные, цилиндровые, кодовые** и **электроиные замки**.

**Бессувальдные** механизмы замков характерны тем, что засовы (ригели) перемещаются в них бороздками ключей. Ригель в каждом замке стопорится подпружиненной собачкой. Секретность бессувальдных замков осуществляют устройства, препятствующие введению в ключевину «чужого» ключа.

**Сувальдные** механизмы замков имеют ригель, сблокированный с пакетом из 3–6 и более подпружиненных сувальд, смонтированных на одной оси. Сувальды представляют собой пластины, имеющие со стороны сопряжения с бороздками ключа разные контуры. Различные секреты образуют сувальды, сложенные вместе пакетом. Им соответствуют в замке профили бороздки ключа.

В **цилиндровых** замках перемещение засова и обеспечение секретности замка достигается за счет его цилиндра. Цилиндр замка содержит комбинацию штифтов и пружин в корпусе цилиндра и в сердечнике (рис. 19.10). В каждом отверстии прижимная пружина воздействует на штифты таким образом, что верхний штифт заходит в соответствующее отверстие в сердечнике и не дает ему проворачиваться. Ключ, вставленный в сердечник, нажимает на соответствующие штифты и совмещает зазор между штифтами корпуса и штифтами сердечника с зазором между сердечником и корпусом цилиндра. В результате этого ключ может повернуть связанный с сердечником кулачок, который перемещает засов замка.

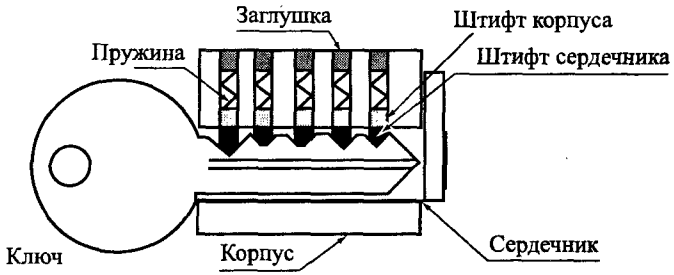



*Рис. 19.10.* Однорядовая цилиндрическая головка

Подобные замки имеют малую замочную скважину и легкий плоский ключ, что упрощает его ношение. Как правило, в конструкции цилиндров предусмотрены вставки из закаленной стали, затрудняющие возможность высверливания штифтов. С целью повышения секретности увеличивают до 2–3 количество рядов штифтов. Очень высокую степень секретности имеют так называемые биаксиальные цилиндровые замки. Их конструкция предусматривает не только утапливание каждого штифта на определенную глубину, но и разворот его на строго определенный для каждого штифта угол.

**Кодовые механические** замки имеют блокиратор ригеля, для разблокировки которого необходимо совпадение заранее установленных цифр кода с цифрами, набираемыми на цифровой панели замка.

В **электронных** замках установка кода, его хранение и сравнение с набираемыми цифрами производятся с помощью микропроцессорной техники, команды которой управляют электромагнитным блокиратором, устанавливаемым в замки любых типов. Микропроцессорная техника позволяет повысить стойкость замка не только за счет увеличения длины кода, но и путем введения других ограничений, например по интервалу времени, в течение которого замок невозможно открыть.

Дверные замки по способу установки делятся на **врезные, накладные** и **навесные**. Врезной замок устанавливается внутрь дверной панели или ящика письменного стола, накладной замок крепится с внутренней стороны двери, дужка навесного замка фиксирует дверь или створки дверей в закрытом состоянии.

Взломостойкость замков зависит от конструкции, типа металла и секретности запорного механизма, оцениваемой количеством комбинаций положений штифтов или кодовых комбинаций. Чем больше количество комбинаций, тем выше его стойкость от различного рода отмычек. В замках с повышенными противовзломными свойствами на запорной планке закрепляются стальные дополнительные планки и вводятся стальные штыри, которые через косяк двери входят в стену. Для защиты от перепиливания в засов запрессовываются закаленные стальные штифты. Например, врезной сувальдный замок «Бизон» (НИЦ «Охрана») имеет 3 пальцевой ригель, выдерживающий поперечное усилие 1500 кг и торцевую нагрузку 500 кг, и секретность свыше 30 млн кодовых комбинаций.

Наибольшую секретность имеют **электронные замки** с ключами в виде электронных карточек «Touch Memory». Электронный ключ этого замка представляет микросхему, размещенную в герметичном корпусе из нержавеющей стали и формирующую 64-разрядную последовательность кода. Корпус имеет цилиндрическую форму диаметром 16 мм и высотой 3–5 мм. Такой корпус устойчив к воздействию агрессивных сред, к влаге, грязи и механическим нагрузкам. Кроме защиты корпус микросхемы выполняет роль контактной группы: один контакт — крышечка и боковая поверхность, другой — изолированное металлическое донышко. Электронный замок срабатывает при совпадении кода, генерируемого ключом, с кодом замка. Секретность такого замка составляет $10^{20}$ комбинаций.

### 20.2.2. Окна

В типовом строительстве в окна вставляют листовое строительное стекло толщиной 2–6 мм, которое обладает слабыми защитными свойствами. Традиционно окна с такими стеклами укрепляются металлическими решетками. Решетки устанавливаются на тех окнах, через которые возможен легкий доступ в помещение здания. К ним относятся, прежде всего, окна на первом или последнем этажах здания, вблизи наружных лестниц или близко расположенных больших деревьев. Металлические решетки бывают бескаркасные, прутья которых заделываются непосредствен-

но в стену, и каркасные — прутья привариваются к металлической раме, а рама затем крепится к стене. Диаметр прутьев не менее 10 мм (обычно 15 мм), расстояние между ними составляет порядка 120 мм, глубина задела их в стену не менее 200 мм.

Другой путь повышения укрепленности окон — защитное остекление с использованием закаленных, армированных, ламинированных, многослойных, органических стекол, стеклопакетов и стеклянных пустотелых блоков.

**Закаленное стекло** в процессе изготовления подвергается специальной термической обработке (нагреву с быстрым охлаждением), в результате которого в стекле образуются остаточные напряжения, обеспечивающие повышенную (приблизительно в 4 раза выше, чем у обычного листового) прочность, стойкость и травмобезопасный характер разрушения. При разрушении закаленное стекло полностью распадается на мелкие (1–2 см) кусочки, причем их размеры обратно пропорциональны степени закалки. Но закаленное стекло разрушается при слабом ударе в точках, соответствующих центрам напряженности.

**Армированные листовые стекла** содержат внутри себя металлическую сетку или проволочную арматуру, создающие повышенную механическую стойкость, огнестойкость и травмобезопасность. Для армирования стекла используют скрученную или сваренную сетку с шестиугольными или квадратными ячейками из стальной термически обработанной проволоки диаметром 0,45–0,55 мм со светлой поверхностью. При разрушении армированных стекол их осколки удерживаются армирующей металлической вставкой. Армированные стекла могут иметь гладкую или узорчатую поверхность. Однако металлическая арматура ухудшает прозрачность стекла и эстетический вид конструкции окна. Поэтому в последнее время армированные стекла не находят широкого применения.

**Ламинированные стекла** появились еще в 20-е годы XX столетия. При их изготовлении на прозрачную полимерную пленку наносили клей и соединяли пленку со стеклом. При ударе ламинированного стекла пленка удерживала осколки, не позволяя стеклу разрушиться целиком. На начальном этапе развития полимерной пленки обладала слабой устойчивостью к механическому воздейс-

твию и быстро мутнела. Технологическим прорывом стало применение пленок с высоким сопротивлением на разрыв и нового синтетического клея, обеспечивающего надежное сцепление на молекулярном уровне пленки со стеклом. Современные ламинированные стекла подразделяются на безопасные (безосколочные), особопрочные и противопожарные. Практически все они являются взаимодополняющими, например, они могут сдерживать распространение пламени в течение не менее 40 мин. Прочность стекла с наклеенной многослойной лавсанной пленкой повышается до 20 раз. Металлизированные пленки применяются для повышения коэффициента экранирования электромагнитных волн окна, тонированные — для предотвращения наблюдения через окно и уменьшения коэффициента пропускания окном ультрафиолетового излучения Солнца. Термозащитные пленки отражают до 78% тепловой энергии, что уменьшает возможность перегрева помещения летом и увеличивает экономию тепла зимой.

**Многослойные листовые стекла** состоят из двух и более стекол, соединенных друг с другом по всей площади прослойками из эластичного органического материала. Широко распространены, особенно на транспортных средствах, ударопрочные трехслойные стекла (два стекла и полимерная пленка между ними), получившие название триплекс (от лат. triplex — тройной). Увеличением числа слоев многослойного стекла можно наращивать его прочность вплоть до обеспечения защиты от прострела пулями современного стрелкового оружия. Кроме того, многослойное стекло нельзя вырезать только с одной стороны, что лишает злоумышленника возможности бесшумно, используя стеклорезы, проникнуть в помещение.

**Органическое стекло** представляет собой прозрачный твердый материал, создаваемый на основе полимеров (полиакрилитов, полистирола, поликарбонатов и др.). Органические стекла по сравнению с листовыми стеклами имеют меньшую плотность и хрупкость, но размягчаются при менее высокой температуре. Они изготовляются в виде листов толщиной 4, 8 и 12 см.

**Стеклопакеты** представляют собой жесткую и прочную конструкцию из 2 или 3 стекол, между которыми вставлены прокладки из перфорированных вставок, содержащих гранулы влагопоглотителя (силикагеля). Силикагель исключает запотевание стекол.

Пространство между стеклами заполняется осушенным воздухом или инертным газом. Механические свойства не полностью герметизированного стеклопакета зависят от размеров и толщины и типа его стекол. Хорошо герметизированный стеклопакет имеет устойчивость к удару приблизительно в 1,5 раза выше за счет амортизирующих свойств воздушной (газовой) прослойки.

**Стеклянные пустотелые блоки** изготовляются в результате сварного соединения двух прессованных коробок из стекла. Полость между стеклами герметичная. Механическая прочность пустотелых блоков оценивается пределом прочности при сжатии с торцов (не менее 15 кг/см$^2$) и сопротивлением ударному воздействию с лицевой стороны (не менее 3 кг/см$^2$). Она зависит от толщины стенок.

По прочности защитное остекление от брошенного предмета (удара) разделяют на классы А1, А2 и А3, по защите от пробивания топором — на классы Б1, Б2 и Б3 в зависимости от того, сколько ударов потребуется, чтобы пробить в стекле размером 900 × 1100 мм четырехугольное отверстие размером 400 × 400 мм. К классу защиты А1 относятся стекла, обеспечивающие устойчивость к одиночному удару с энергией до 141 Дж, А2 — с энергией 262 Дж, 3-го класса — 382 Дж. К классу стойкости Б1 относится стекло, выдерживающее 30–50 ударов топором, к классу Б2 — 51–70 ударов, к классу Б3 — более 70 ударов.

## 20.3. Металлические шкафы, сейфы и хранилища

Металлические шкафы предназначены для хранения документов с невысоким грифом конфиденциальности, ценных вещей, небольшой суммы денег. Надежность шкафов определяется только прочностью металла и секретностью замка.

Для хранения особо ценных документов, вещей, больших сумм денег применяются сейфы и хранилища. К сейфам относятся двустенные металлические шкафы с тяжелыми наполнителями пространства между стенками, в качестве которых используются армированные бетонные составы, композиты, многослойные заполнители из различных материалов.

Хранилище представляет собой сооружение с площадью основания внутреннего пространства более 2 м$^2$, защищенное от взлома и устойчивое к воздействию высокой температуры при пожаре.

По конструктивному исполнению хранилища могут быть:

- монолитными;
- сборными;
- сборно-монолитными.

Монолитные железобетонные хранилища при толщине защитных стен более 100 см размещаются в подвале здания на его фундаменте. На междуэтажном перекрытии здания устанавливаются более легкие сборные (модульные) хранилища из тонкостенных конструкций, состоящих из стальной обшивки и заполнителя из высокопрочного армированного бетона.

В соответствии со стандартом ГОСТ Р-50862-96 стойкость хранилищ и сейфов измеряется в условных единицах сопротивления ($E_c$), которые оцениваются временем взлома с учетом коэффициента мощности применяемого инструмента. Различают взлом с полным доступом, когда открывается дверь сейфа или хранилища, и частичным доступом. Взлом с частичным доступом предполагает создание в сейфе отверстия, достаточного для просовывания в него руки. Каждому инструменту, используемому при взломе, приписывается определенный коэффициент: чем мощнее инструмент, тем больше коэффициент и меньше время взлома. Например, для различных зубил этот коэффициент равен 1–5, для электродрели — 5, а для газового резака — 7,5.

Весь интервал единиц стойкости (30–4500 $E_c$) разделен на 13 классов устойчивости взлому. Группу самой высокой стойкости образуют хранилища 11–13 классов (2000–4500 $E_c$). Время взлома их при использовании самого эффективного инструмента (электрорежущего инструмента с алмазным буром мощностью до 11 кВт, газовых горелок и др.) должно быть не менее 45–120 мин. Это время не учитывает время для определения зоны воздействия, выбора и смены инструмента, мер по соблюдению взломщиком мер осторожности, например по снижению шума. Реальное время превышает «чистое» время, равное времени непосредственного контакта инструмента с сейфом, в 3–4 раза.

**Сейфы** имеют меньшую взломоустойчивость, чем хранилища. Сейфы с высокой устойчивостью характеризуются 7–10 классами (400–1350 $E_c$). Например, для частичного доступа к сейфу V класса с использованием лома, кувалды и зубила требуется в среднем

22 мин, газового резака — 14,1 мин, а колонкового бура с алмазной коронкой — 8,7 мин [8].

Взломоустойчивость сейфа в значительной степени зависит от стойкости замков. Замки для сейфов делятся на ключевые, кодовые механические и электронные. Чаще в сейфах используются сувальдные ключевые замки, которые лучше цилиндровых защищены от взлома. Недостаток ключевых замков — возможность утери или копирования ключей. Этого недостатка лишены механические кодовые замки. Но они нуждаются в высокой точности установки диска на соответствующие деления. При ошибке на пол деления время доступа к вложению увеличивается за счет повторного набора кода. Электронные кодовые замки лишены этих недостатков. Кроме того, они обеспечивают возможность быстрой смены кода; задержки времени на открывания, подключения к пульту охраны. Но они являются энергозависимыми и их можно вывести из строя специальными электрическими сигналами.

Дополнительно отдельные хранилища испытываются на устойчивость к взлому с использованием взрывчатых веществ с массой заряда до 500 г в тротиловом эквиваленте. Выдержавшее испытание хранилище маркируется дополнительным индексом «ВВ».

Сейфы оцениваются также на пожаро- и влагоустойчивость. Устойчивость сейфа к температуре характеризуется временем, в течение которого температура внутри сейфа не превысит температуру возгорания бумаги или других вложений. В соответствии с отечественным стандартом сейфы по пожароустойчивости делятся на 3 класса. Сейф класса Б обеспечивает защиту бумажных вложений от возгорания, температура которого составляет около 170° С. Внутренняя температура сейфа класса Д не должна превышать температуры деформации магнитных пленок 70° С. Сейфы класса ДИС предназначены для хранения винчестеров и дискеток с температурой до 50° С. Максимальное время защиты вложений пожароустойчивых сейфов может достигать 4 ч, но наиболее распространены сейфы с временем устойчивости 1–2 ч.

Сейфы для хранения машинных носителей оцениваются также временем непревышения внутри сейфов значений предельной влажности 80–85% при 100% влажности окружающей среды.

Сейфы высокого класса имеют большой вес, который надо учитывать при выборе места их установки, особенно для слабых межэ-

тажных перекрытий. Для затруднения выноса легких сейфов вместе с содержимым они крепятся к полу или вделываются в стену.

При выборе сейфов рекомендуется учитывать:

- объем и тип вложения (деньги, документы, машинные носители, материальные ценности);
- вид воздействия (взлом, огонь, вода);
- количество и типы замков сейфа;
- масса-габаритные характеристики, влияющие на способ установки сейфа (на полу без крепления, с креплением к полу, в стене);
- максимальная сумма страхового покрытия в случае взлома сейфа, которая изменяется в значительных пределах в зависимости от класса сейфа.

На основе практики считается, что ущерб от взлома минимален, если цена сейфа составляет около 10% цены вложений.

## 20.4. Средства систем контроля и управления доступом

Средства систем контроля и управления доступом включают:

- устройства ввода идентификационных признаков;
- устройства управления;
- исполнительные устройства (управляемые преграждающие устройства).

Устройства ввода идентификационных признаков считывают их с идентификаторов. Возможны следующие способы ввода признаков:

- ручной, осуществляемый путем нажатия клавиш, поворота переключателей и т. д.;
- контактный в результате непосредственного контакта между считывателем и идентификатором;
- дистанционный (бесконтактный) при поднесении идентификатора к считывателю на определенное расстояние.

В качестве атрибутных идентификаторов людей используются удостоверения, постоянные, временные и разовые пропуска, а в последнее время — идентификационные карты. Для идентификации транспорта применяются государственные номера, устанавливаемые на транспортном средстве, и их технические паспорта. Внос

(ввоз) и вынос (вывоз) груза производится по путевым листам, материальным пропускам и идентификационным картам. В качестве идентификаторов допуска в здание, помещение, шкаф, хранилища, сейф используются ключи замков, закрывающих и открывающих соответствующие двери.

Удостоверение представляет собой документ, подтверждающий принадлежность конкретного лица к организации, выдавшей удостоверение, а пропуск — документ на право допуска в организацию или в отдельные контролируемые зоны. Удостоверения и постоянные пропуска выдаются сотрудникам на срок не менее года, временные — на срок выполнения задания в организации или на испытательный срок поступающим на работу, разовый пропуск — посетителям организации на один день. В удостоверение и постоянный пропуск вписывают фамилию, имя, отчество, другие реквизиты, наклеивается фотография лица, наносятся условные знаки, обозначающие, в том числе, контролируемые зоны, в которые разрешен доступ. Подлинность удостоверения и постоянного пропуска подтверждается подписью должностного лица и печатью организации. Временный пропуск со сроком действия более 1 месяца также имеет фотографию, остальные пропуска действительны при предъявлении паспорта или удостоверения личности. В разовом пропуске указывается время выдачи и ухода. Вход в организацию разрешается в течение не более 30 минут после его получения, а задержка с уходом — не более 15 минут.

Удостоверения и пропуска имеют слабую защиту от подделки. Поэтому постоянные пропуска каждый год перерегистрируются и через несколько лет меняют на новые, с измененным внешним видом. Во время перерегистрации и после утери пропуска сотрудником на пропуск наносятся дополнительные буквенные, цифровые или графические знаки.

В большинстве автоматизированных КПП в качестве атрибутов доступа применяются идентификационные карточки. Карточка представляет собой пластиковую пластину стандартизированного размера, которая наряду с набором традиционных реквизитов ее владельца (фамилии, имени, отчества, фотографии) содержит скрытый персональный идентификационный номер и другие данные, необходимые для его достоверного опознавания средствами автоматизации.

В зависимости от способа записи идентификационной информации карточки делятся на следующие виды:

- магнитные, с записью информации о полномочиях владельца карточки на полоске магнитного материала на одной из ее сторон. Считывание информации производится путем перемещения карточки в прорези считывающего устройства;
- инфракрасные, изготавливаемые из прозрачного для ИК-лучей пластика. На внутреннюю поверхность слоя пластика наносится с помощью вещества, адсорбирующего ИК-лучи, идентификационный номер владельца. Атрибуты владельца считываются при перемещении карточки вдоль щели измерителя признаков в ИК-лучах внешнего источника;
- штриховые, в которых штриховой код наносится на один из внутренних слоев карточки и считывается путем перемещения карточки в прорези терминала;
- карточки «Виганд» (по имени американского исследователя J. R. Weigand), в пластиковую основу которых впрессовываются две полоски из коротких проводников, располагаемых в строго определенной для каждой карты последовательности. Каждая последовательность образует персональный код владельца карты. Считыватель содержит индукционную катушку с двумя магнитами противоположной полярности. При проведении карты по считывателю полоски создают в катушке индукционные отклики положительной и отрицательной полярности, образующие бинарный PIN-код;
- бесконтактные «проксимити» (proximty) карты, номер с которых считывается без непосредственного контакта со считывателем (на расстоянии 10–150 см). Основу карты составляет микросхема с энергонезависимой памятью и рамочная антенна, размещенные внутри герметизированной пластиковой карты. В пластиковой карте размера кредитной размещена электронная схема радиочастотного идентификатора. Идентификатор посылает считывателю закодированный сигнал, на основе которого принимается решение о допуске. В зависимости от источника питания применяют два вида карт: активные и пассивные. Карты «проксимити» с батарей питания обеспечивают работу на значительно больших расстояниях, чем пассивные, но они более

дорогие, имеют увеличенную толщину, менее надежны. В качестве источников электропитания пассивных карт используется радиоприемник карты, аккумулирующий электромагнитную энергию, излучаемую высокочастотным генератором считывателя.

Результаты качественного сравнения магнитных карт, карт Виганда и Проксимити указаны в табл. 20.3.

*Таблица 20.3*

| *Показатели карты* | *Характеристика типа карты* | | |
|---|---|---|---|
| | *Виганд карта* | *Проксимити* | *Магнитная карта* |
| Скрытность кода | высокая | средняя | низкая |
| Возможность изменения кода | нет | нет | есть |
| Пропускная способность | средняя | высокая | низкая |
| Время жизни карты | большое | большое | малое |
| Время жизни считывателя | большое | среднее | малое |
| Влияние электромагнитных полей | отсутствует | высокое | высокое |
| Стоимость эксплуатации | низкая | средняя | высокая |

Наименее защищенными от фальсификации считаются магнитные карточки, наиболее защищенными — карты Виганда и проксимити. Карты Виганда имеют высокие надежность и устойчивость к внешним воздействиям, невысокую стоимость карт и считывателя, их практически невозможно подделать. Когда необходимы высокая пропускная способность, скрытность установки считывателя и возможность дистанционной идентификации, целесообразно применение проксимити карт.

Достоинства биометрических идентификаторов вызвали интенсивное развитие соответствующих средств. В качестве биометрических идентификаторов используются:

- рисунок папиллярных линий пальцев;
- рисунок радужной оболочки глаз;
- рисунок капилляров сетчатки глаз;
- тепловое изображение лица;
- геометрия руки;
- динамика подписи;

- особенности речи;
- ритм работы на клавиатуре.

С целью идентификации личности по **рисунку папиллярных линий пальца** проверяемый набирает на клавиатуре свой идентификационный номер и помещает указательный палец на окошко сканирующего устройства. При совпадении получаемых признаков с эталонными, предварительно заложенными в память ЭВМ и активизированными при наборе идентификационного номера, подается команда исполнительному устройству. Хотя рисунок папиллярных линий пальцев индивидуален, использование полного набора их признаков чрезмерно усложняет устройство идентификации. Поэтому с целью его удешевления применяют признаки, наиболее легко измеряемые автоматом. Выпускают сравнительно недорогие устройства идентификации по отпечаткам пальцев, действие которых основано на измерении расстояния между основными дактилоскопическими признаками. На величину вероятности ошибки опознания влияют также различные факторы, в том числе температура пальцев. Кроме того, процедура аутентификации у некоторых пользователей ассоциируется с процедурой снятия отпечатков у преступников, что вызывает у них психологический дискомфорт.

При идентификации личности по **рисунку радужной оболочки и капилляров сетчатки глаз** производится сканирование с помощью оптической системы радужной оболочки и сетчатки одного или обоих глаз. Радужная оболочка глаза содержит большое количество именных признаков человека. При идентификации по сетчатке глаза измеряется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и другие признаки. Всего насчитывают около 250 признаков. Такие биометрические терминалы обеспечивают высокую достоверность идентификации, сопоставимую с дактолоскопией, но требуют от проверяемого лица фиксации взгляда на объективе сканера.

Устройства идентификации личности по **геометрии руки** находят широкое применение, так как ее трехмерное изображение содержит достаточный для надежной идентификации объем информативных признаков и обеспечивает быстрый анализ. Но признаки руки меняются с возрастом, а само устройство имеет сравнительно большие размеры.

Устройства идентификации по **динамике подписи** используют геометрические или динамические признаки рукописного воспроизведения подписи в реальном масштабе времени. Проверяемому лицу предлагается написать свою фамилию или другое слово на специальной пластине, преобразующей изображение слова в эквивалентный электрический сигнал с последующим измерением характеристик письма, начертания подписи, интенсивности каждого усилия при написании букв и быстроты завершения написания.

Среди признаков лица, используемых для идентификации человека, наиболее устойчивыми и трудно изменяемыми являются **признаки изображения его кровеносных сосудов**. Путем сканирования изображения лица в инфракрасном свете создается уникальная температурная карта лица — **термограмма**. Идентификация по термограмме обеспечивает показатели, сравнимые с показателями идентификации по отпечаткам пальцев.

Идентификация по **ритму работы на клавиатуре** основана на измерении временных интервалов между двумя последовательными ударами по клавишам при печатании знаков.

Средства биометрических идентификаторов обеспечивают очень высокие показатели идентификации: вероятность несанкционированного доступа — 0,1–0,0001%, вероятность ложного задержания — доли процентов, время идентификации — единицы секунд, но имеют более высокую стоимость по сравнению со средствами атрибутной идентификации. Качественные результаты сравнения различных биометрических технологий по точности идентификации и затратам указаны на рис. 20.1 [9].

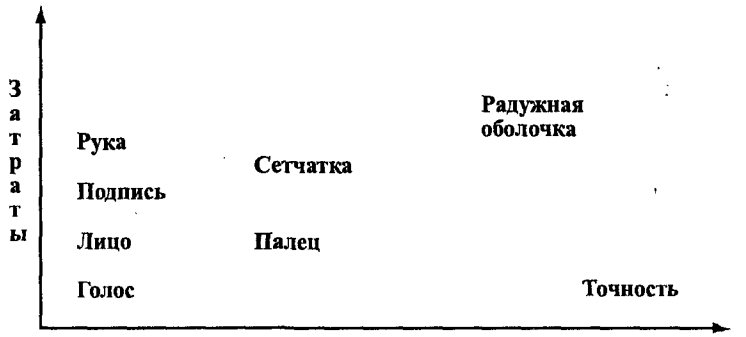



*Рис. 20.1.* Сравнение методов биометрической идентификации

Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах управления доступом.

Управляемые преграждающие устройства (УПУ) различаются по назначению и конструкции. Для управления доступом в организации применяют **турникеты и шлюзовые кабины (шлюзы)**, в помещение — **двери с электромагнитными и электромеханическими замками**, открываемые вручную и автоматически.

**Турникеты** различаются по виду перекрытия зоны прохода и способу управления ими. По виду перекрытия они могут быть с частичным или полным перекрытием. По способу управления турникеты могут быть снабжены ручным (ножным), полуавтоматическим и автоматическим управлением.

Турникеты бывают «нормально открытые» и «нормально закрытые», а также поясные и в полный рост. Нормально открытые, например раздвижные турникеты в Московском метро, имеют более высокую пропускную способность, но применяются реже, чем нормально закрытые, так как вызывают у проходящих через них людей психологический дискомфорт из-за боязни получить удар закрывающимися створками, а также не исключают возможность прохода нескольких прижавшихся друг к другу человек.

Наиболее распространены трехлопастные турникеты с вращающимся в одном направлении преграждающимся устройством — триподы и роторные. Они обеспечивают гарантированный единовременный проход одного человека. Преграждающее устройство триплода выполнено в виде вращающегося блока с тремя цилиндрическими брусьями (штангами), расположенными под углом 120°. Вращающийся блок крепится сбоку зоны прохода. При вращении каждый из брусьев фиксируется в горизонтальном положении, преграждая путь человеку. Роторные турникеты высотой до пояса человека (поясные) и в полный рост (полноростовые) обеспечивают полное перекрытие зоны прохода. Так как через заградительный барьер поясного турникета можно перелезть или перепрыгнуть, он размещается на посту охраны и управляется нажатием на его педаль ногой вахтера.

Турникеты обеспечивают высокую пропускную способность до 60 человек в минуту, дешевле шлюзовых кабин, но их конструкция не мешает задерживаемому применить против сотрудников охраны оружие. Кроме того, размеры пространства между заградительными барьерами устанавливаются исходя из размеров человека средней комплекции, что создает неудобства для толстяков и при проносе крупногабаритных носимых вещей. Для повышения эффективности защиты турникеты оснащаются датчиками, срабатывающих при нерегламентированном поведении человека, например попытке перепрыгнуть через заграждающий барьер.

Для систем управления доступом с высоким уровнем защиты применяют УПУ закрытого типа — **шлюзовые кабины**. Шлюзовая кабина тамбурного типа представляет собой закрытую конструкцию с двумя дверьми, которые одновременно не открываются. После прохода человека в шлюз входная дверь закрывается, проводится его идентификация и по разрешающей команде вахтера или контролера СКУД открывается выходная дверь, расположенная уже на территории организации. В случае отказа на допуск обе двери блокируются для выяснения службой безопасности личности находящегося в шлюзе человека. Шлюзовые кабины другого типа — ротанты имеют вращающиеся двери с тремя или четырьмя лопастями или образующие два сектора.

Шлюзовые кабины могут быть полуавтоматические и автоматические. В полуавтоматических шлюзовых кабинах применяются распашные двери, которые открываются вручную и закрываются доводчиком, но блокируются с помощью электромагнитных или электромеханических замков, управляемых вахтером или контролером. В автоматических шлюзовых кабинах двери открываются и закрываются с помощью электромеханических приводов, управляемых контролером СКУД или вахтером. В отличие от полуавтоматических шлюзов в автоматических шлюзах применяются двери различных конструкций: одностворчатые и двустворчатые распашные двери, раздвижные двери с плоскими или полукруглыми створками, складывающиеся двери, цилиндрические двери, одностворчатые и двустворчатые двери с плоскими поворачивающими створками.

В шлюзовые кабины устанавливаются считыватели и другие средства биометрической идентификации. Закрытая конструкция шлюза оказывает психологическое давление на человека, стремящегося проникнуть на территорию организации без надежных документов. Двери и стены шлюзов, как правило, выполняются из ударопрочного стекла (бронестекла) или пластика. Часто в шлюзы встраиваются датчики металлодетектора и других средств контроля вносимых или выносимых вещей, прежде всего оружия, взрывчатых и радиоактивных веществ.

Элементы турникетов, преграждающие путь злоумышленнику, могут подвергаться механическим воздействиям, особенно во время его задержания. Турникеты и шлюзовые кабины по механической устойчивости делятся так же, как двери, на УПУ нормальной, на повышенной и высокой устойчивости.

Так как преграждающие устройства могут подвергаться разрушающим и неразрушающим воздействиям злоумышленников, то их по механической устойчивости стандарт классифицируется следующим образом:

- повышенная устойчивость к взлому посредством нанесения ударов и применения инструментов;
- высокая устойчивость, характеризуемая пуле- и взрывоустойчивостью сплошного перекрытия проходного проема.

Кроме того, в СКУД предусматриваются меры по обеспечению устойчивости к вскрытию злоумышленниками замков и запорных механизмов, по предотвращению наблюдения за вводом идентификационных признаков и копирования эталонных признаков идентификаторов.

Контрольно-проездные пункты для пропуска авто- и железнодорожного транспорта оборудуются:

- раздвижными или распашными воротами и шлагбаумами с механическим, электромеханическим и гидравлическим приводами, а также устройствами для аварийной остановки ворот и открывания их вручную;
- контрольными площадками с помостами для просмотра автомобилей;
- светофорами, предупредительными знаками и световыми табло типа «Берегись автомобиля» и др.;

- телефонной и тревожной связью и освещением для осмотра автотранспорта.

Традиционная (неавтоматическая или с автоматизированным приводом дверей) система контроля управления доступом транспорта включает ворота или шлагбаумы для пропуска и задержания транспорта, площадку с помостом для осмотра транспорта, которая часто представляет собой участок проезжей части дороги, светофор, предупредительные знаки, световые табло, оповещающие окружающих о выезде и въезде транспорта, а также средства сигнализации, освещения и тревожной связи контролера, осматривающего транспортное средство. Ворота могут быть **распашными**, с невысокой стойкостью против тарана и требующими очистки проезжей части перед воротами от снега и льда, **раздвижные, подъемные и рулонные**. В качестве атрибутных идентификаторов на транспортное средство применяют путевой лист, в котором указывается государственный номер машины, фамилия водителя и лица, ответственного за перевозку груза (часто эти функции выполняет водитель), вид и количество груза. Идентификаторами водителя и пассажиров являются их пропуска.

Современные СКУД транспорта оснащаются также дистанционными атрибутными идентификаторами (идентификаторами типа Proximity), средствами досмотра транспорта (специальными зеркалами и техническими эндоскопами), а также на особо важных объектах — антитеррористическим средством для экстренной остановки автомобиля, пытающегося протаранить ворота. Последнее средство представляет собой металлическую колонну (блокиратор) диаметром до 50 см, которая устанавливается перед воротами с внешней стороны в бетонированном или металлическом колодце. На дне колодца размещается баллон со сжатым воздухом и пиропатроном, который взрывается по электрическому сигналу с КПП, а сжатый воздух поднимает колонну за доли секунд перед движущимся автомобилем. Подобный блокиратор может остановить 20 тонный автомобиль, движущийся со скоростью 60 км/час.

Обработку всей информации и управление преграждающими устройствами осуществляют средства вычислительной техники (микропроцессоры и компьютеры).

**Вопросы для самопроверки**

1. Классификация ограждений по назначению. Типы заборов, устанавливаемые по периметру организации.
2. Средства укрепления заборов.
3. Способы и средства укрепления прочности дверей.
4. Типы замков, применяемых для закрытия дверей.
5. Средства укрепления окон, преимущества ламинированных стекол.
6. Типы хранилищ, отличия хранилищ от сейфов.
7. Классификация устройств идентификации.
8. Типы исполнительных механизмов. Преимущества биометрических идентификаторов.

# Глава 21. Средства технической охраны объектов

## 21.1. Средства обнаружения злоумышленников и пожара

Средства обнаружения злоумышленника и пожара составляют ядро комплекса охраны источников информации и других ценных объектов, так как от вероятности обнаружения вторжения и оповещения о нем сил нейтрализации зависит эффективность нейтрализации угроз. Одним из основных средств обнаружения и пожара являются извещатели.

### 21.1.1. Извещатели

Разнообразие видов охраняемых зон и их характеристик привело к многообразию видов и типов извещателей. Классификация их дана на рис. 21.1.

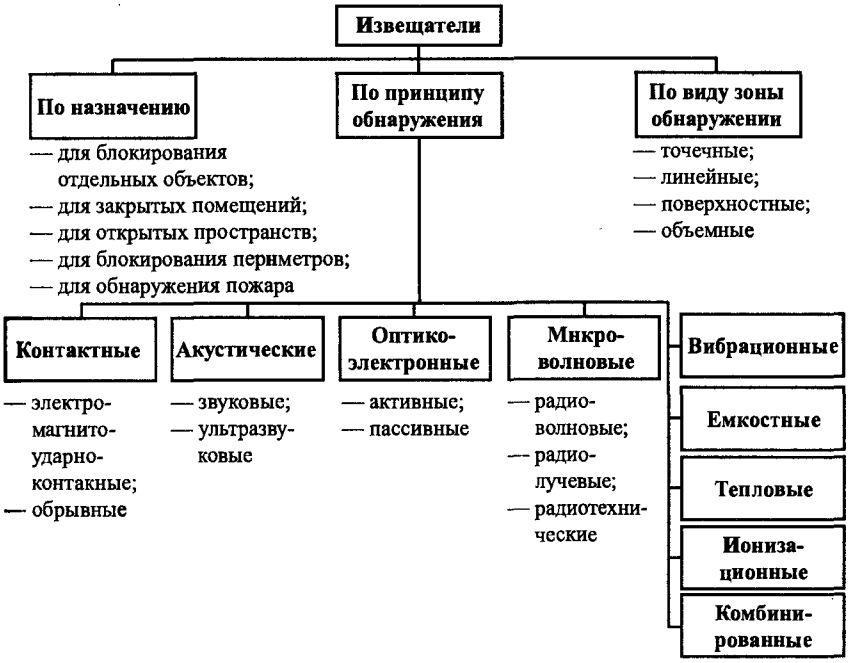



*Рис. 21.1.* Классификация извещателей

По назначению извещатели делятся на средства для **блокирования отдельных объектов, обнаружения злоумышленника и пожара в закрытых помещениях, обнаружения нарушителя на открытых площадках и блокирования периметров территории, здания, коридора**. Такое деление обусловлено особенностями указанных зон и требованиями к средствам обнаружения в этих зонах. Средства охраны помещений и открытых площадок должны обнаруживать злоумышленника в любой точке этих зон, периметровые — при пересечении им периметра зоны. К средствам для охраны закрытых помещений предъявляются менее жесткие требования по устойчивости средств к климатическим воздействиям, но ограждения помещения вызывают многочисленные переотражения излучаемых извещателями полей, и эти особенности необходимо учитывать при создании и грамотной эксплуатации соответствующих средств.

По виду охраняемой зоны средства обнаружения делятся на **точечные, линейные, объемные и поверхностные**. Точечные средства обеспечивают охрану отдельных объектов, линейные — периметров, поверхностные — стен, потолков, окон, витрин и др., объемные — объемов помещений или открытых площадок.

По принципу обнаружения злоумышленника и пожара извещатели разделяют на:

- контактные;
- акустические;
- оптико-электронные;
- микроволновые (радиоволновые);
- вибрационные;
- емкостные;
- тепловые (пожарные);
- ионизационные (пожарные);
- комбинированные.

**Контактные извещатели** реагируют на механические действия (открывание двери, люка или окна, пролом стены, давление веса), приводящие к замыканию или размыканию контактов извещателя, а также к обрыву тонкой проволоки или полоски фольги. Они бывают электроконтактными, магнитоконтактными, ударноконтактными и обрывными.

**Электроконтактные извещатели** (ДЭК-3, СК-1М, БК-1М и др.) представляют собой выключатели, которые под действием механической силы (при открытии злоумышленником двери, оконной рамы, форточки, шкафа и др.) размыкают или замыкают электрические цепи, соединяющие извещатели с приемно-контрольным прибором. Электроконтактые извещатели могут быть закамуфлированы под коврик перед дверью. Такой коврик представляет собой два металлических листа, между которыми проложен пористый диэлектрик с отверстиями. Листы с прокладкой помещают в оболочку из пластика или водонепроницаемой ткани и накрывают материалом типового коврика. Под тяжестью злоумышленника листы замыкаются через отверстия в диэлектрике, что приводит к возникновению сигналов тревоги.

**Магнитоконтактные датчики** (СМК-1 (ИО 102-2), СМК-3, ДМК-П, ИО102-4, 5, 6, 15, 16 и др.) предназначены для блокирования открывающихся поверхностей (дверей, окон, люков и др.), а также переносимых предметов (экспонатов музеев и выставок). Извещатель содержит геркон (герметичную стеклянную трубку с укрепленными внутри магнитоуправляемыми контактами) и постоянный магнит, размещенных в одинаковых пластмассовых корпусах прямоугольной или цилиндрической формы. Магнит крепится на подвижной части блокируемой поверхности или на музейном экспонате, геркон — на неподвижной части или на подставке экспоната параллельно магниту на удалении не более 6–8 мм. Когда дверь, окно, люк закрыты, а экспонат находится на подставке, расстояние между магнитом и герконом минимальное, магнит притягивает контакты геркона и в зависимости от типа извещателя их замыкает или размыкает. При открывании злоумышленником поверхности или хищении экспоната магнит удаляется от геркона и контакты меняют свое положение на противоположное. Возникает сигнал тревоги.

**Ударноконтактные датчики** («Окно-4», «Окно-5», «Окно-6» (ИО-303-6), УКД-1М, ВМ-12М, ДИМК и др.) обеспечивают блокирование поверхностей, прежде всего, оконных стекол, разрушающихся от удара. Принципы работы основаны на замыкании или размыкании электрических контактов во время их колебаний после удара по стеклу, к которому приклеен корпус датчика. Один кон-

такт извещателя прикреплен к его корпусу, на конце другого, упругого контакта укреплен массивный груз. В силу инерционности этого груза гибкий контакт при колебаниях корпуса практически не изменяет своего положения, в результате чего он замыкается или размыкается с движущимся вместе с корпусом другим контактом. В современных ударноконтактных извещателях предусмотрен винт для регулировки чувствительности извещателя к удару. Изменением чувствительности минимизируются ложные срабатывания извещателя для конкретной помеховой обстановки.

Основу **обрывных извещателей** составляют тонкий провод, алюминиевая фольга и токопроводящий слой стекла или пленки. Провода диаметром 0,1–0,25 мм применяются для блокировки деревянных и прочих некапитальных конструкций помещения, решеток окон, небольших временных стоянок. Провод прокладывается по всей внутренней блокируемой поверхности параллельными рядами с расстоянием между рядами проволоки не более 200 мм, заделывается внутрь или вокруг стержней решеток окон, навешивается на кусты и деревья на высоте около 1 м вокруг охраняемой стоянки. Блокировку внутренних металлических решеток производят путем обвивания горизонтальных и вертикальных прутьев проводом с шагом витка 30–70 мм. Провод, уложенный на поверхности, маскируют шпаклевкой с последующим окрашиванием или покрывают листовым материалом (оргалитом, фанерой и др.).

Обрывные извещатели «Трос-1», «Кувшинка» и «Трепанг», применяемые для охраны мест временного расположения людей, техники, грузов, различных объектов и территории, обеспечивают блокирование рубежа максимальной протяженности 1,5, 2 и 5 км соответственно. Контакт между проводами после обрыва восстанавливается путем сплавления концов проводов при помощи спички или зажигалки.

Фольга алюминиевая толщиной 0,008–0,015 мм и шириной 6–10 мм применяется в основном для блокирования остекленных поверхностей площадью не более 8 м$^2$. Например, извещатель «Фольга-С» комплектуется самоклеящейся фольгой шириной 10 мм, толщиной 14 мкм и длиной 5–20 м. Фольга наклеивается по периметру стекла на удалении нескольких мм от рамы и закраши-

вается краской под цвет рамы или фона стеклянной поверхности. К фольге крепится шлейф в виде гибкого провода (ПМВГ-0,2 или аналогичного).

Обрывные извещатели имеют высокую помехоустойчивость и широко применяются для блокирования поверхностей (на пролом и стекла на разбивание) и периметров.

**Акустические извещатели** для обнаружения злоумышленника используют акустические волны в звуковом и ультразвуковом диапазонах, которые возникают при разрушении им механических преград или отражаются от нарушителя при проникновении его в охраняемое помещение. Акустические извещатели, реагирующие на акустические сигналы при разрушении злоумышленником блокируемой поверхности, являются пассивными, ультразвуковые извещатели излучают акустические волны и являются активными.

Пассивные акустические извещатели («Грань-1, 2», « Шорох-1», «Гюрза-050М», «Окно-1» и др.) применяются для защиты строительных конструкций (окон, витрин, стен, потолков, полов, сейфов и др.). В них внешний акустический сигнал, возникающий при разбитии и взломе, преобразуется в электрический. При соответствии текущих признаков акустического сигнала эталонным формируется сигнал тревоги.

Для преобразования акустических сигналов в электрические применяют в основном поверхностные и воздушные пьезоэлектрические и электромагнитные датчики. Мембрана поверхностного датчика крепится (приклеивается) к защищаемой поверхности, воздушные акустические извещатели воспринимают воздушные акустические волны.

С целью уменьшения вероятности ложных тревог от акустических помех увеличивается количество используемых для идентификации демаскирующих признаков и усложняются алгоритмы их обработки. Например, поверхностный пьезоэлектрический извещатель «Грань-2» выдает сигнал тревоги при наличии трех признаков: определенной амплитуды вибрации корпуса извещателя, приклеенного к блокируемой поверхности, уровня и числа импульсов от разрушительных воздействий за время 15 с. В перспективном бесконтактном извещателе о разбитии стекла «Арфа» производится цифровая двухканальная обработка акустических сигналов

микропроцессором по 5 признакам разбития стекла. В звуковом извещателе «Class Tech» (Visonic Ltd) реализована так называемая технология компьютерного распознавания акустического образа (КРАО). Звуки, обнаруженные электретным микрофоном, преобразуются в цифровые сигналы, которые обрабатываются процессором. Трехэтапный статистический анализ и процесс принятия решения используют 18 различных признаков для надежного отличия настоящих тревог от ложных.

**Ультразвуковые** датчики (ДУЗ-4, ДУЗ-4М, ДУЗ-5, ДУЗ-12, «Фикус-МП-2», «Эхо-2», «Эхо-3» и др.) генерируют сигнал тревоги при появлении злоумышленника в контролируемой зоне охраняемого помещения. Извещатель содержит излучатель акустической волны в ультразвуковом диапазоне, приемник (акустоэлектрический преобразователь) и электронный блок обработки. Излучатель посылает в охраняемое помещение акустическую волну с частотой выше 23 кГц. В результате интерференции прямых и отраженных волн в помещении возникают «стоячие» волны. При появлении в помещении человека, а также пламени пожара изменяется конфигурация отражающих поверхностей и характер «стоячих волн», а следовательно, изменяется уровень акустического сигнала на входе приемника, что приводит к появлению сигналов тревоги на выходе электронного блока. Снижение влияния помех достигается регулировкой чувствительности приемника. На таком принципе работают извещатели типа ДУЗ. Однопозиционный извещатель ДУЗ-12 обеспечивает охрану помещения объемом 0,3–150 м$^3$. Извещатель ДУЗ-4М допускает подключение до 3 пар излучатель-приемник и позволяет защитить одновременно до трех помещений общим объемом до 2000 м$^3$, а ДУЗ-5 обеспечивает работу до 10 пар и охрану до 5 помещений общим объемом до 5000 м$^3$.

С целью снижения влияния акустических помех в более современных ультразвуковых извещателях предусмотрена селекция акустического сигнала по величине изменения его частоты в соответствии с эффектом Допплера. Эффект Допплера проявляется в изменении частоты сигнала, отраженного от движущейся поверхности. Если поверхность удаляется от источника звука, то частота уменьшается, когда приближается — частота увеличивается. В приемнике извещателя в результате измерения изменения часто-

ты принимаемого акустического сигнала относительно частоты излучаемого выявляется отраженный от движущегося человека сигнал на фоне других сигналов, отраженных от неподвижных предметов. Для уменьшения ложных срабатываний необходимо также учитывать следующие требования по установке акустических извещателей:

- высота установки — 1,5...2,5 м от пола;
- не допускается установка извещателя непосредственно над батареями отопления, около форточки или фрамуги, вблизи оконных штор, декоративных растений и других предметов, колеблющихся под действием воздушных потоков в помещении;
- на период охраны должны быть закрыты все окна, форточки и фрамуги, отключена принудительная вентиляция и калориферы, выключены или отключены любые источники акустических сигналов (телефоны, электрические звонки, репродукторы и т. д.).

В **оптико-электронных извещателях** для обнаружения злоумышленника и пожара используются инфракрасные лучи. По принципу действия такие извещатели делятся на активные и пассивные. Активные инфракрасные излучатели состоят из одной или нескольких пар излучателя ИК-лучей и фотоприемника. Сигнал тревоги формируется при пересечении ИК-луча злоумышленником.

Излучатель активного оптико-электронного извещателя создает узкий луч света в ИК-диапазоне, который в дежурном режиме освещает его фотоприемник. При пересечении луча злоумышленником или появлении на пути его распространения дыма уровень сигнала на выходе фотоприемника резко уменьшается, что приводит к формированию сигнала тревоги. В литературе активные оптико-электронные извещатели называют также фотоэлектрическими. В качестве источников излучения используются лампы накаливания, размещаемые в кожухе с отражателем и закрытые прозрачными для ИК-лучей фильтрами, и светодиоды, излучающие свет в ИК-диапазоне. В качестве светочувствительных элементов приемника применяются фотодиоды и фототранзисторы.

Так как излучатели создают узкие лучи в ИК-диапазоне, то активные оптико-электронные излучатели используются в основном для блокирования длинных поверхностей — коридоров, стен, за-

боров, периметров территории и зданий, т. е. выполняют функции линейных извещателей. С целью повышения надежности блокирования создают несколько параллельных лучей с помощью средств, в комплект которых входит соответствующее количество пар излучатель-фотоприемник. Например, активный оптико-электронный извещатель «Мак» создает до 16 лучей. Количество параллельных лучей может быть увеличено также переотражением луча с помощью входящих в состав некоторых извещателей отражателей. Оптико-электронные излучатели с отражателями применяют для блокирования дверных и оконных проемов. Если укрепить на внутренней стороне двери отражатель, а излучатель и приемник устанавливаются рядом на верхней части дверной рамы, то сигнал тревоги возникает не только при пересечении злоумышленником луча, но и при открывании двери. Например, применяемые для этого извещатели ДОП-1,2 обеспечивают длину блокируемой поверхности 0,4–2,5 м, а ДОП-3 — 0,5–5 м.

Оптико-электронные извещатели используются также для обнаружения пожара, сопровождаемого обильным образованием дыма. Дым может ослабить луч извещателей, применяемых для блокирования поверхностей до уровня, при котором происходит формирование сигнала тревоги. Специальные пожарные извещатели постоянно контролируют оптическую плотность воздуха возле потолка помещения. Пожарный извещатель имеет полость, в которой установлены излучающий светодиод и фотодиод приемника. При попадании внутрь оптической камеры частиц дыма рассеянный ими ИК-свет освещает фотодиод. Срабатывание извещателей с выдачей сигнала «Пожар» происходит при задымлении среды, снижающей ее прозрачность на 0,05–0,2 дБ/м.

Пересечение лучей активных оптико-электронных извещателей мелкими животными, птицами, листьями или другим мусором при сильном ветре, а также атмосферные осадки (сильный туман, ливень, снегопад) могут вызвать ложные тревоги. С целью их уменьшения модулируют луч при его излучении и вводят при формировании сигнала тревоги задержку на время перекрытия луча, называемую чувствительностью к перекрытию луча.

Модуляция луча осуществляется путем подачи на излучатель импульсного питающего напряжения. Например, в извеща-

теле «Мак» длительность излучения составляет 30 мкс с частотой повторения 50 Гц. Демодуляция сигнала в приемнике производится синхронным детектором, на выходе которого возникает сигнал при несовпадении информационных и опорных сигналов. В качестве опорного сигнала для детектора используется последовательность импульсов, модулирующая луч и передаваемая от излучателя к приемнику по дополнительному проводному или радиоканалу синхронизации. Ложная тревога в этом случае возникает при совпадении времени прерывания светового импульса помехой с временем его излучения, что маловероятно. Действительно, при использовании извещателя «Мак» и равной вероятности по времени появления помехи в зоне луча вероятность ложной тревоги составляет величину, равную отношению времени излучения светового импульса к периоду импульсной последовательности, т. е. порядка 0,015.

Для уменьшения этой величины при формировании сигнала тревоги учитывается время прерывания луча злоумышленником и помехой. Даже бегущий человек не может прервать луч на время менее 0,1–0,5 с. Введение временной задержки устраняет влияние на работу извещателя мелких быстродвижущихся животных и птиц.

Сочетание рассмотренных способов позволяет существенно снизить вероятность ложных тревог. Кроме того, при установке извещателя в месте эксплуатации необходимо также учитывать принципы их работы и исключить попадание в зону действия луча качающихся от ветра штор в помещении и веток деревьев на открытом пространстве, прямого солнечного света и света автомобильных фар.

Пассивные оптико-электронные извещатели формируют сигнал тревоги при попадании на вход термочувствительного элемента ИК-излучений от злоумышленника или от очага пожара. Эффективность работы пассивного извещателя тем выше, чем больше разность между температурой источника тепла и температурой фона. При разнице менее (2–3)° С извещатель «слепнет», т. е. электрический сигнал в блоке обработки, соответствующий тепловому излучению злоумышленника или пожара, не отличается от помех.

В современных пассивных ИК приборах применяется схема автоматического увеличения чувствительности пропорционально росту температуры в помещении, но при этом может также увеличиться вероятность ложной тревоги. В зависимости от типа оптики извещатель имеет различные зоны обнаружения: от одно-лучевой длиной до 50 м и углом обзора 10–50 градусов до почти объемной, состоящий из 3–5 «вееров» по 10–16 лучей в каждом. Извещатель с зоной обзора в виде конуса с углом обзора около 70 градусов («Квант-3») устанавливается на потолке помещения и применяется для охраны экспонатов музеев. Диаграмма зон обнаружения формируется оптической системой извещателя на основе зеркал или линз Френеля. Современные извещатели комплектуются несколькими видами сменной оптики. Например, в извещателях «Фотон-1М, 2» формируется несколько чувствительных зон в одной плоскости. «Фотон-4» способен формировать зону обнаружения, состоящую из 32 чувствительных лучей в вертикальной и горизонтальной плоскостях. «Фотон-5» создает две сплошные вертикальные чувствительные зоны большой площади, позволяющие с высокой вероятностью обнаруживать источники тепла. В извещателе «Фотон-6» путем использования сменных линз Френеля могут создаваться 3 вида зон обнаружения: вертикальная типа «занавес», объемная в виде многоуровневых секторов и узкая типа «коридор».

Так как пассивные оптико-электронные извещатели чувствительны к любым ИК-излучениям, в том числе батарей отопления, кондиционеров, к солнечным лучам, то с целью снижения вероятности ложной тревоги в извещателях сигнал тревоги формируется при последовательном пересечении источником ИК-излучений чувствительных зон. С учетом этого извещатель нужно устанавливать в помещении таким образом, чтобы исключалось движение злоумышленника к объекту защиты в створе луча. При выборе места размещения извещателей в помещении необходимо также руководствоваться следующими соображениями:

- извещатель не должен освещаться солнцем, особенно если перед окном имеются деревья, крона которых может создавать блики;
- извещатель не следует устанавливать так, чтобы он или стена на противоположной стороне охраняемого участка освещались дальним светом автомобильных фар;

извещатель не следует располагать на расстоянии менее 1,5 м от вентиляционного отверстия и батареи центрального отопления.

Повышенная помехоустойчивость по отношению к помехам в видимом и ИК-диапазонах света достигается также использованием для обнаружения очагов горения открытым пламенем датчиков ультрафиолетового излучения и цифровой обработки сигналов от фотоприемника. Примерами таких извещателей могут служить пожарные извещатели ИП329-2 («Аметист») и ИП 329-1 («Пламя»).

**Микроволновые (радиоволновые) извещатели** используют для обнаружения злоумышленников электромагнитные волны в СВЧ диапазоне (9–30 ГГц). Они содержат СВЧ генератор, приемник и передающие и приемные антенны. Так как на электромагнитное поле в СВЧ диапазоне не влияют акустические помехи, свет и в существенно меньшей степени атмосферные осадки, то эти извещатели все более широко применяются для охраны помещений, открытых пространств и периметров.

В зависимости от вида электромагнитного поля микроволновые излучатели делятся на **радиолучевые** и **радиотехнические**.

В радиолучевых извещателях для блокирования периметров («Радий-1», «Пион-Т (ТМ)», «Риф-РЛ», «Гарус», «Лена-2», «Протва», «Витим») антенна излучателя формирует узкую диаграмму направленности в виде вытянутого эллипсоида с высотой и шириной в середине зоны обнаружения 2–10 м. Длина одного участка обнаружения достигает 300 м. При пересечении человеком электромагнитного луча, излучаемого передающим устройством в сторону приемника, уменьшается из-за экранирующих свойств человека напряженность поля в точке приема, в результате чего возникает сигнал тревоги.

Радиоволновые объемные извещатели формируют объемную зону обнаружения, заполняющую электромагнитным полем весь объем помещения. Для снижения мощности излучения, что важно для безопасности обслуживающего персонала и повышения помехоустойчивости, в современных извещателях предусматривается импульсный режим работы. Кроме того, для уменьшения ложных тревог в схеме объемных извещателей реализуется принцип селекции на основе эффекта Допплера.

Радиотехнические извещатели обнаруживают злоумышленника по изменениям им характеристик СВЧ поля. Электромагнитное поле создается одним или несколькими СВЧ передатчиками. В качестве передающий антенны применяется специальный радиочастотный кабель, прокладываемый вдоль периметра охраняемой территории. Антенна приемника размещается в центре территории или в виде кабеля, параллельного передающему. При вторжении злоумышленника в чувствительную зону извещателя характеристики сигнала на входе приемника изменяются, что вызывает сигнал тревоги.

Способ обнаружения злоумышленника с помощью размещаемой в центре охраняемой территории антенны приемника реализован в быстро развертываемой радиотехнической системе «Виадук»», предназначенной для обнаружения вторжения в охраняемую зону злоумышленников, двигающихся ползком, согнувшись или в полный рост со скоростью 0,5–6 м/с. Передающий радиочастотный кабель располагается по периметру на расстоянии 150–300 м от антенны приемника.

В извещателе «Бином» (Россия) и «S-Trax» электромагнитное поле создается между двумя параллельно проложенными коаксиальными кабелями с отверстиями. Кабели укладываются по периметру блокируемой территории в землю на глубине 10–15 см и на расстоянии 2–3 метров друг от друга. Из отверстий кабеля, подключенного к генератору, «вытекает» электромагнитное поле и «втекает» в отверстия кабеля, подключенного к приемнику. Кабели этих извещателей создают зону обнаружения шириной до 10 м и высотой и глубиной около 70 см. Закапывание кабелей в землю позволяет применять этот извещатель для обнаружения подкопа, обеспечивает его хорошую маскировку, высокую помехоустойчивость от транспорта, однако на чувствительность этого извещателя влияет электропроводность грунта.

К **вибрационным** относятся извещатели, обнаруживающие злоумышленника по создаваемой им вибрации в грунте при движении, в легком заборе (типа сетки «рабица») при попытке преодоления его нарушителем, при открывании дверей, окон, люков и др. конструкций. Вибрационные извещатели отличаются от акус-

тических инфразвуковым диапазоном воспринимаемых ими частот колебаний блокируемой поверхности. В зависимости от физической природы преобразования механического давления в электрический сигнал вибрационные извещатели бывают электретные, магнитные, волоконно-оптические, трибоэлектрические. Если датчики извещателя размещаются в грунте, то вибрационные извещатели называют также сейсмическими.

В вибрационных извещателях чувствительные элементы выполняются в виде отдельных (пьезо- и электромагнитных) датчиков, кабелей и шлангов с жидкостью. В электретных и трибоэлектрических кабелях создается электрическое поле, в кабелях типа «Guardwire 400» — магнитное поле, в световодах — световой луч. Датчики укрепляются на защищаемой поверхности, кабели навешиваются на проволочные заборы, ими опутываются ручки дверей, люков, краны трубопроводов, шланги закапываются в грунт. В результате механических воздействий нарушителя на чувствительные элементы вибрационных извещателей в них возникают электрические сигналы (в электромагнитных, магнитных, пьезоэлектрических, трибоэлектрических, электретных) или изменяются характеристики светового сигнала. Изменение давления в любой точке шланга жидкостного извещателя, вызванное вибрацией, передается к гидрофону, преобразуется в электрический сигнал, который при превышении заданного уровня вызывает сигнал тревоги. Сигнал тревоги возникает также при попытках разрушения злоумышленником кабелей.

Для надежной селекции сигналов, вызванных злоумышленником, от помех производится постоянно усложняемая в новых типах извещателей обработка сигналов от чувствительных элементов. Например, в периметровом волоконно-оптическом извещателе «Ворон» (Московский технический университет связи и информатики, АО «Рефлектор») повышение помехоустойчивости достигается применением 4 канального процессора, обучаемого после монтажа на конкретном объекте с имитацией пересечения нарушителем заграждения.

**Емкостные извещатели** («Ромб-К4», «Пик», «Барьер-М», «Риф», «Градиент» и др.) создают сигналы тревоги при приближе-

нии злоумышленника к объекту охраны. С точки зрения радиотехники движение злоумышленника можно представить как приближение токопроводящей поверхности достаточно большой площади, являющейся моделью злоумышленника, к токопроводящей поверхности антенны емкостного извещателя, размещенной на объекте охраны. В качестве антенны может быть использована токопроводящая поверхность охраняемого объекта (например, сейфа) или электрический провод, укрепляемый в оконных или дверных проемах, шкафах, на стенах складов и т. д. Между человеком и антенной существует распределенная емкость, величина которой обратно пропорциональна расстоянию между ними. Принцип работы емкостных извещателей состоит в изменении эквивалентной (собственно контура и распределенной) емкости контура генератора сигналов извещателя, вызванной увеличением распределенной емкости между приближающимся нарушителем и антенной извещателя. Изменение емкости приводит к изменению частоты генератора и уменьшению амплитуды связанного с ним контура, настроенного на частоту генератора при отсутствии вблизи антенны человека. Несовпадение частот в контурах приводит к снижению амплитуды колебаний во втором контуре, уменьшение которой менее порога вызывает сигнал тревоги. Чувствительность емкостных датчиков оценивается максимальным расстоянием приближения к антенне, которое составляет 10–30 см.

Для обнаружения пожара применяются извещатели, реагирующие на демаскирующие признаки пожара — повышенную концентрацию дыма в воздухе, высокую температуру и излучения открытого пламени. В различных условиях эти демаскирующие признаки имеют разную информативность.

На повышение температуры в помещении реагируют **тепловые извещатели**. Тепловые извещатели применяют в помещениях, в которых при возгорании быстро повышается температура воздуха. Тепловые извещатели делят на максимальные и дифференциальные. Максимальные подают сигнал тревоги при превышении значения температуры воздуха температуры срабатывания извещателя.

В качестве чувствительных к температуре элементов в них применяются:

- терморезисторы, уменьшающие свое сопротивление при повышении температуры;
- термобиметаллические пластины с разными коэффициентами теплового расширения, изгибаемые и размыкающие электрические контакты при повышении температуры;
- легкоплавкие сплавы (Вуда с температурой плавления 60,5°С, д'Арсе — 79°С), замыкающие при нормальной температуре контакты извещателя;
- термоферриты с уменьшающейся с повышением температуры магнитной проницаемостью и используемые в качестве сердечников электромагнитных реле, которые размыкают контакты при снижении магнитного поля менее уровня срабатывания реле.

В извещателях с терморезисторами уменьшение сопротивления приводит к увеличению силы протекающего через них тока. При превышении его значения заданного (эталонного) возникает сигнал тревоги. Изменяя эталонное значение силы тока, можно настроить извещатель на требуемую максимально допустимую температуру.

Максимальные тепловые извещатели имеют достаточно большую инерционность (30–90 с), обусловленную временем нагревания чувствительного элемента до температуры срабатывания.

Меньшую инерционность и большую устойчивость к изменениям внешней среды имеют дифференциальные тепловые извещатели. Дифференциальный извещатель содержит два чувствительных элемента, один из которых (внешний) контактирует с воздухом среды, а другой — внутренний, размещен внутри корпуса извещателя и непосредственного контакта с окружающей средой не имеет. Сигналы с каждого из чувствительных элементов подаются на входы дифференциального усилителя. Сигнал на выходе этого усилителя пропорционален разности входных сигналов. Когда температура обоих чувствительных элементов одинакова, то сигнал на выходе усилителя близок к нулю. Медленное повышение температуры воздуха в помещении из-за, например, жаркой погоды не изменяет уровень сигнала на выходе дифференциального усилителя. При быстром изменении температуры воздуха нагревание чувствительных элементов происходит с разной скоростью. В ре-

зультате этого входные сигналы отличаются по величине, уровень сигнала на выходе усилителя увеличивается, что приводит к формированию сигнала тревоги.

Так как дым является наиболее информативным признаком пожара и, что особенно важно, на начальном этапе возгорания, когда нет еще открытого пламени, то наиболее широко применяются пожарные извещатели, реагирующие на дым. По принципам работы различают оптические и ионизационные извещатели. В **оптическом извещателе** измерительная камера с отверстиями для поступления воздуха содержит ИК-излучатель (светодиод) и фотоприемник (фотодиод), расположенные друг против друга. При отсутствии в воздухе дыма свет от излучателя попадает на фотоприемник почти без затухания. При задымленности воздуха световой поток на элементе фотоприемника уменьшается, сигнал на его выходе снижается до порогового значения.

В **ионизационных извещателях** вместо света используется поток радиоактивного слабого излучения частиц плутония-239 со сверхнизкой излучающей активностью 10 мкКю и америций-241 с активностью 0,8–0,9 мкКю. Поток радиоактивных излучений направляется в 2 камеры. В измерительную камеру проходит окружающий воздух, а контрольная камера изолирована от воздуха. При отсутствии дыма в измерительной камере разность сигналов на выходах детекторов мала. В случае появления дыма в ней интенсивность потока снижается, разность уровней сигналов детекторов возрастает, возникает сигнал тревоги. Ионизационные извещатели относятся к наиболее надежным пожарным датчикам, их конструкция обеспечивает полную радиационную безопасность. Но их не рекомендуется устанавливать в детских учреждения, школах, жилых помещениях и других местах, где они могут быть изъяты и разобраны детьми или чрезмерно любопытными взрослыми. Кроме того, после окончания срока эксплуатации (более 5 лет) ионизационных извещателей необходимо захоронение содержащихся в них радиоактивных веществ. Качественное сравнение ионизационных и оптических извещателей при различных видах горения приведены в табл. 21.1 [10].

*Таблица 21.1*

| *Вид горения* | *Способ обнаружения* | |
|---|---|---|
| | *Ионизационный* | *Оптический* |
| Открытое горение древесины | + | – |
| Тление древесины | – | + |
| Тление хлопка | + | + |
| Открытое горение пластмассы | + | + |
| Горение жидкости с выделением сажи | – | + |
| Горение керосина | + | – |

Указанные извещатели являются точечными и используются в основном для помещений типовой конфигурации. Для обнаружения возгораний в длинных и узких помещениях или конструкциях (кабельных каналах, транспортных депо, химических реакторах и др.) применяют линейные тепловые извещатели и традиционные периметровые инфракрасные извещатели.

Линейный тепловой извещатель представляет собой кабель, содержащий 4 медных проводника, каждый из которых покрыт оболочкой из материала с отрицательным температурным коэффициентом. Оболочки проводников в кабеле плотно прижаты друг к другу. Концы проводников попарно соединены друг с другом, образуя две петли. Сопротивление между петлями зависит от сопротивления оболочек, значение которой изменяется при изменении их температуры. Блок обработки линейного теплового извещателя формирует сигнал тревоги при снижении этого сопротивления менее заданного значения.

Периметровые инфракрасные извещатели реагируют на повышение величины затухания среды за счет ее задымленности так же, как реагируют они на пересечение луча злоумышленником.

Однако не все виды возгораний, особенно на начальном этапе, сопровождаются интенсивным выделением дыма. Для обнаружения пламени используются ультрафиолетовые и инфракрасные извещатели пламени. Ультрафиолетовый извещатель представляет собой высоковольтный газоразрядный датчик с чувствительностью в области ультрафиолетового диапазона (220–280 мкм).

Ультрафиолетовые лучи от открытого пламени ионизируют газ между электродами датчика и увеличивают ток разряда, что используется в устройстве обработки для формирования сигнала тревоги. Оптические инфракрасные извещатели реагируют на излучение открытым пламенем пожара инфракрасных лучей, аналогичных инфракрасному излучению человеком.

Многообразие видов пожара и их демаскирующих признаков вынуждает разработчиков пожарных извещателей к созданию комбинированных извещателей, срабатывающих на различные признаки разных видов пожара.

Основной проблемой при создании и применении извещателей остается обеспечение высокой вероятности обнаружения злоумышленника (для охранных извещателей) и пожара (для охранно-пожарных и пожарных извещателей) и малой вероятности ложных срабатывания. Для исключения психологического привыкания охранников к ложным тревогам, которое негативно отражается на их отношении к службе, ложное срабатывание не должно происходить чаще одного раза в течение 1–2 тысяч часов.

Повысить надежность обнаружения злоумышленника или пожара можно путем дублирования извещателей с разными принципами обнаружения. Но при простом дублировании одновременно возрастает вероятность ложных тревог, так как приемно-контрольный пункт реагирует на сигнал тревоги, в том числе ложный, от каждого извещателя. Для повышения вероятности обнаружения злоумышленника и пожара при малых значениях вероятности ложной тревоги в **комбинированных извещателях** усложняется алгоритм обработки сигналов от разных датчиков.

В периметровых комбинированных извещателях «Протва-3, 4» вибрационный извещатель навешивается на забор, под ним зону обнаружения формирует радиолучевой извещатель, а в грунт укладывается радиотехнический извещатель типа «Бином». В комбинированном извещателе для охраны особо протяженных периметров «Гоби» предусмотрена возможность комплектации различными видами датчиков: контактными, вибрационными, радиолучевыми, емкостными и др.

### 21.1.2. Средства контроля и управления средствами охраны

**Приемно-контрольные приборы (ПКП)** обеспечивают:

- одновременный прием сигналов тревоги от извещателей с подачей световой и звуковой сигнализации;
- передачу сигналов тревоги на пульт централизованного наблюдения;
- возможность увеличения емкости за счет добавления к базовому составу линейных блоков;
- автоматический переход на резервное автономное питание в случае выключения основного;
- формирование сигналов оповещения операторов в случае обрыва или короткого замыкания шлейфов.

ПКП классифицируются по информационной емкости (количеству подключаемых шлейфов) и информативности (количеству видов извещателей). По информационной емкости они бывают малой емкости (до 5 шлейфов), средней (6–50 шлейфов) и большой емкости (свыше 50 шлейфов). ПКП малой информативности обеспечивают работу до 2 видов извещателей, средней — от 3 до 5 видов извещателей. Преимущественно они используются для охраны одного объекта.

При создании ПКП проявляется тенденция расширения на базе микропроцессоров их функциональных возможностей в части автоматизации контроля за состоянием извещателей, адаптации к их различным характеристикам, совершенствования алгоритмов обработки.

Например, в ПКП «Буг» предусмотрена возможность программирования параметров прибора с учетом особенностей подключаемых шлейфов, мажоритарная обработка сигналов, защита от попыток несанкционированного доступа к его элементам и повреждения линий связи.

В современных ПКП средней и большой емкости предусматривается возможность передачи извещений на пульты централизованного наблюдения по отдельному каналу связи.

**Пульты централизованной охраны** предназначены для централизованного приема, обработки и индикации информации с объектов охраны. Они обеспечивают:

- контроль состояния охраняемого объекта;
- взятия объекта под охрану и снятие с охраны;
- автоматическое переключение аппаратуры АТС на средства охраны;
- регистрацию нарушения шлейфов охраняемых объектов с указанием номера объекта и характера нарушения;
- световую индикацию номеров объекта, где произошло нарушение.

Состояние объекта охраны определяется по типу передаваемого от него извещения и по признакам состояния («норма», «замыкание», «обрыв») абонентской линии между объектом и пунктом централизованной охраны. Короткое замыкание или обрыв вызывают изменения тока в линии, в результате чего выдается сигнал тревоги с звуковой сигнализацией и световой индикацией номера объекта.

Для **передачи извещений и команд управления** на пульт централизованного наблюдения используются линии телефонной связи, специальные проводные линии, радиоканалы, комбинированные линии связи.

Передача извещений по телефонным линиям связи производится в комплексах «Центр-КМ», «Нева-10»», «Нева-10М», «Прогресс-ТС», «Атлас-2М», «Фобос» и др., обеспечивающих обслуживание от 30 до 400 и более охраняемых объектов.

Для централизованной охраны не телефонизированных объектов применяются радиосистемы передачи извещений «Струна-2» и «Струна-3». Они состоят из пульта централизованного наблюдения с приемником и объектовых блоков с передатчиками в диапазоне частот 166,7–166,95 МГц. По радиоканалу передается 8 видов извещений: «снят», «взят», «проникновение-вход», «проникновение-периметр», «пожар», «вызов», «авария». Радиосистема «Струна-2» предназначена для охраны до 7 пространственно разнесенных объектов, удаленных от пункта охраны до 3 км, а «Струна-3» — до 160 объектов на удалении до 3 и 6 км (при использовании направленных передающих и приемных антенн).

В автоматической системе тревожной сигнализации по линиям городской телефонной сети «Циклон» автоматизируются про-

цессы взятия под охрану и снятия с охраны. Вся тревожная и служебная информация (время, номер объекта, вид извещения) автоматически фиксируется. В системе предусмотрена работа с 4 АТС и обслуживание до 1000 номеров.

## 21.2. Средства телевизионной охраны

Основными средствами телевизионной охраны являются **телевизионные камеры** и **мониторы**.

Обычное разрешение аналоговых **телевизионных камер** для видеоконтроля составляет для черно-белых 380–450 ТВЛ и цветных меньше — 300–320 ТВЛ, в системах высокого разрешения применяют камеры с повышенной четкостью, равной 500–600 и 375–450 линиям соответственно. Для обычного формата кадра (размеров по вертикали и горизонтали) 3 : 4 изображение при разрешении 400 ТВЛ состоит из 1200000 пикселей.

Спектральная характеристика ПЗС матриц по сравнению с характеристикой глаза сдвинута в сторону более длинных лучей и захватывает инфракрасную область. Поэтому при инфракрасной подсветке возможно видеонаблюдение, незаметное для злоумышленника. Эта особенность телевизионных камер на ПЗС камерах используется для создания ловушек злоумышленнику, который, выбирая для движения темные места, попадает в зону видеонаблюдения.

Камеры обычной чувствительности позволяют наблюдать в сумерках, при освещенности 0,1–0,5 лк для черно-белых камер и 1–3 лк для цветных камер, а камеры высокой чувствительности — в условиях лунной ночи (порядка 0,01 лк).

Для обеспечения приемлемого качества изображения в широком диапазоне освещенности объекта, в том числе мерцающем свете газоразрядных ламп, телевизионные камеры системы видеонаблюдения оснащаются дополнительными устройствами: электронным затвором, автоматической диафрагмой (автоирисом), автоматической регулировкой усиления сигналов ПЗС-матрицы, гамма-коррекции, компенсации засветки и внешней синхронизации.

Так как для дежурного освещения все чаще используются газоразрядные лампы, мигающие с частотой питающего напряжения 50 Гц, то при наблюдении с помощью телевизионных камер,

частота кадровой синхронизации которых отличается от частоты сети, возникает стробоскопический эффект. Он заключается в том, что на экране монитора в последовательные моменты времени наблюдаются разные части изображения, которые зрительная система оператора интерпретирует как движущееся изображение в вертикальном направлении со скоростью, соответствующей разности мигания освещения и кадровой развертки камеры. Кроме того, при последовательном подключении нескольких камер с разной частотой кадровой развертки к монитору в его блоке синхронизации возникает переходной процесс подстройки под частоту подключаемой камеры. В течение этого процесса на экране монитора наблюдается искаженное хаотическое изображение, утомляющее оператора. Для исключения этих явлений к блоку синхронизации камеры подаются **сигналы внешней синхронизации** от питающей сети или внешнего синхронизатора коммутатора или мультиплексора.

По конструктивному признаку телевизионные камеры делятся на **корпусные и бескорпусные**. Бескорпусные телевизионные камеры имеют малые габариты и устанавливаются в различных бытовых предметах для скрытого наблюдения. Камеры для открытого наблюдения размещаются в защитных кожухах. Кожухи камер, устанавливаемых в отапливаемых помещениях, имеют разнообразную конструкцию, обеспечивающую установку на стене, в углу помещения или на потолке. Защитные свойства кожухов классифицируются в соответствии с международным стандартом двухразрядным номером. Первая цифра в интервале 0–6 указывает на степень защиты кожуха от проникновения посторонних предметов (твердых тел диаметром от 1 мм до 50 мм, песка, пыли), вторая (в интервале 0–8) — от проникновения воды. Кожухи камер, применяемые на открытом воздухе, имеют прочный («вандалоустойчивый») корпус и устойчивое к удару стекло окошка перед объективом. Шлицы винтов на кожухе имеют нестандартную форму или спиливаются. Для работы в широком диапазоне климатических условий они герметизируются, на них укрепляется солнцезащитный козырек, в них оборудуется подогрев. Некоторые кожухи имеют дополнительное оборудование — вентиляторы, дворники, омыватели стекла. Кожухи наружного наблюдения для исключения возможности изменения злоумышленником ориентации каме-

ры жестко закрепляются на стенах, столбах и других конструкциях по возможности на большой высоте (4–5 м).

Для осмотра пространства территории или помещения с помощью средне- и длиннофокусных объективов телевизионные камеры устанавливаются на дистанционно управляемых поворотных платформах с углом поворота в горизонтальной плоскости до 350 градусов и до 180 градусов в вертикальной плоскости. Если в процессе наблюдения наряду с получением панорамных изображений требуется рассматривать детали объектов наблюдения, то используются объективы с переменным фокусным расстоянием, управляемые с пульта оператором.

Аналоговые телевизионные камеры со временем будут вытеснены цифровыми камерами, в которых видеосигнал на выходе ПЗС оцифровывается и вся последующая обработка производится с сигналами в цифровой форме.

В простейшем варианте видеосигналы с телекамеры непосредственно подаются на вход монитора по коаксиальному электрическому кабелю. При размещении телевизионных камер на большом расстоянии от монитора передача видеосигнала может осуществляться по радиоканалу.

**Мониторы**, так же как и телекамеры, делятся на черно-белые и цветные. Они имеют размер экрана 7, 9, 12, 14, 15, 17, 21 дюйм и разрешающую способность выше разрешающей способности телевизионных камер. При использовании в системе видеоконтроля обычных черно-белых камер используют мониторы с разрешением 500–800 ТВЛ, для цветных — 300–400 ТВЛ. В системах высокого разрешения применяют черно-белые мониторы с разрешением 900–1000 ТВЛ, цветные — 450–500 ТВЛ.

Основным элементом монитора, определяющим его размеры, разрешающую способность, цветовую гамму, яркость и контраст изображения, является электронно-лучевая трубка (кинескоп), жидко-кристаллическая или плазменная панели.

ЖК-мониторы имеют по сравнению с мониторами на ЭЛТ ряд преимуществ:

- не излучают опасные электромагнитные поля, что существенно повышает скрытность информации, отображаемой на экране;
- отсутствуют вредные для здоровья излучения (рентгеновские, электрические, магнитные, электромагнитные);

- не чувствительны к внешним магнитным полям;
- более полно используется видимая поверхность экрана (поверхность экрана 15-дюймовых ЖК-мониторов соответствует поверхности 16-дюймовых мониторов на ЭЛТ);
- имеют равномерное разрешение экрана по всей поверхности;
- отсутствует дрожание изображения по вертикали;
- значительное (на 40–50%) меньшее энергопотребление, большая компактность и меньший вес.

Но ЖК-мониторы пока проигрывают мониторам на ЭЛТ по яркости и насыщенности красок цветного изображения, углу его обзора и цене.

Лучшими яркостными характеристиками обладают мониторы на плазменных панелях. Яркость и контрастность плазменных панелей сопоставимы с аналогичными характеристиками электронно-лучевых трубок, но они имеют меньшие габариты, массу, больший срок службы и излучают вредные электромагнитные поля существенно меньшего уровня. Преимущества плазменных панелей особенно ощутимы при создании больших экранов. Поэтому прослеживается тенденция постепенной замены мониторов на ЭЛТ на жидкокристаллические, а в будущем — на плазменные.

По мере увеличения количества установленных телевизионных камер возникает необходимость в повышении числа мониторов. Однако при установке на рабочем месте охранника более 4–6 мониторов у него во время наблюдения быстро наступает психологическая усталость, особенно при использовании мониторов с электронно-лучевыми трубками. Так как дрожание изображения на них становится особенно заметным в периферической области зрения, то при увеличении количества мониторов возрастает вредное влияние дрожания изображения на зрение. Поэтому для охранного телевидения предпочтительными являются более дорогие мониторы с частотой кадровой развертки в 100 Гц.

С целью снижения нагрузки на оператора и повышения эффективности видеоконтроля применяют **видеокоммутаторы, видеоквадраторы, мультиплексоры, детекторы движения, специальные видеомагнитофоны** и так называемые **видеоменеджеры** на базе компьютеров.

Современные **видеокоммутаторы** делятся на коммутаторы последовательного действия и матричные видеокоммутаторы.

Видеокоммутаторы последовательного действия подключают несколько (4–20) телекамер к одному монитору с последовательным автоматическим «листающим» и ручным режимами работы, позволяющие просматривать изображения всех камер или выборочно от некоторых из них. В современных коммутаторах предусматриваются: регулировка времени просмотра изображения каждой камеры; входы для сигналов тревоги от извещателей для быстрого подключения к монитору сигналов от ближайшей к извещателю камеры; «залповый» режим, который позволяет наблюдать участки охраняемой зоны, на каждом из которых устанавливаются нескольких камер. Видеокоммутаторы последовательного действия являются простыми устройствами с ограниченными возможностями и постепенно вытесняются матричными видеокоммутаторами с существенно большим набором функций.

Матричные видеокоммутаторы имеют встроенный процессор и обеспечивают дополнительно к функциям последовательных видеокоммутаторов вывод на экран монитора: изображений от камер в любом порядке с управлением их поворотными устройствами и вариообъективами, номеров камер и названий помещений, в которых они установлены, сообщений о сигналах тревоги, текущего времени, даты, инструкции оператору и др. Указанные функции позволяют создавать гибкие и наращиваемые системы охраны объектов защиты.

**Видеоквадраторы (разделители экранов)** уменьшают количество используемых мониторов путем одновременного показа на одном экране монитора нескольких изображений (4 и более). При этом экран делится на части по количеству телекамер. Различают видеоквадраторы «реального времени», обеспечивающие смену изображений одновременно на всех квадратах экрана монитора, и видеоквадраторы последовательного типа с последовательным переключением изображений в квадратах. Квадраторы имеют также дополнительные (по количеству камер) тревожные входы для подключения средств сигнализации, обеспечивают вывод на полный экран изображения от соответствующей камеры, остановку кадра, передачу сигналов тревоги на другие средства и запись на видеомагнитофон.

**Видеомультиплексоры** — устройства, выполняющие временное мультиплексирование, первоначально создавались для обеспе-

чения записи видеосигналов от нескольких (до 16) камер на одну видеокассету и непрерывное воспроизведение видеосигналов одной камеры. Современные дуплексные и триплексные мультиплексоры обладают широкими функциональными возможностями, в том числе позволяют просматривать на экране мониторов изображения от одних камер и записывать на видеомагнитофон сигналы от других камер. Записанные изображения могут просматриваться в полноэкранном формате, режимах квадрированного экрана, «картинки в картинке» и мультиэкрана. Многие мультиплексоры имеют дополнительные функции, в том числе: двухкратного увеличения воспроизводимого изображения и просмотра ранее сделанных записей одновременно с текущей записью изображений с работающих камер, встроенные детекторы движения, генераторы титров, даты и времени. Широкий набор встроенных функций и возможность программирования микропроцессора с помощью функциональных клавиш или клавиатуры персонального компьютера позволяют использовать мультиплексор как устройство управления до 256 камер системы видеоконтроля.

**Видеодетектор движения** представляет собой автономный или встроенный в мультиплексор электронный блок, который запоминает текущий кадр изображения, сравнивает его с последующим и выдает сигнал тревоги при несовпадении сравниваемых изображений. Различают аналоговые и цифровые детекторы движения. В аналоговых детекторах сравниваются уровни сигналов одинаковых элементов изображения. При попадании в зону наблюдения объекта, отсутствующего на предыдущем изображении, изменяются соответствующие яркости элементов его изображения и уровни сигналов. Если эти изменения превышают установленный порог, детектор движения выдает сигнал тревоги. Введение порога снижает вероятность ложных тревог из-за электрических помех или природных явлений в зоне наблюдения (дождя, снега и др.). Сигнал тревоги подается при превышении этой разности более порогового значения.

В цифровых извещателях создаются предпосылки для существенного повышения помехоустойчивости путем введения в память микропроцессора участков изображения, изменения в которых вызывают сигнал тревоги. Для этого поле изображения разделяет-

ся на большое количество ячеек, из которых составляют участки сравнения произвольной конфигурации. В эти участки не включаются, например, качающиеся ветви деревьев, пол, помещения, по которому могут пробегать грызуны и другие объекты, не связанные с злоумышленником или его действиями. В ряде видеодетекторов можно задавать программным путем также характеристики прогнозируемого движения злоумышленника: начало, направление и скорость движения человека, время суток и др. Например, все входящие в помещение люди вызывают сигнал тревог, а выходящие — нет. Видеодетектор в виде автономного блока может быть сопряжен с любым средством системы видеоконтроля.

Для регистрации и документирования изображений видеокамер применяются **специализированные видеомагнитофоны**, которые в отличие от бытовых обеспечивают существенно большую длительность записи: от 24 часов до 40 суток. Увеличение продолжительности записи достигается за счет записи с пропуском кадров (Time-laps recording), с уплотненной записью и записью по тревоге.

Наиболее распространенный вариант — записывается не каждый кадр, а выборочно. В видеомагнитофоне с длительностью до 24 часов записывается каждый 8-й кадр, а в варианте наиболее длительной записи — каждый 320-й кадр. Но при этом способе речь не записывается. На каждом кадре регистрируется дата и время, что позволяет с точностью до минут восстановить события в случае возникновения нештатных ситуаций. По тревоге может осуществляться также переход из медленных «time-lapse» режимов в один из более быстрых, вплоть до номинальной скорости.

В видеомагнитофонах с уплотненной записью устанавливаются уменьшенные видеоголовки и применяются видеокассеты с улучшенными характеристиками. За более продолжительную запись, например до 12 часов с тройной плотностью на одну кассету, приходится платить ухудшением качества записи и несовместимостью со стандартом VHS.

В магнитофонах с записью по тревоге для обеспечению малого времени от подачи сигнала «Запись» до начала записи предусмотрен режим ожидания. В этом режиме лента видеокассеты заправлена, а видеоголовка постоянно вращается. Для исключения про-

тирания ленты вращающейся головкой лента медленно продвигается со скоростью 6 полукадров за 3 мин.

Современные методы M-JPEG сжатия цифрового видеосигнала в 15–25 раз без ухудшения качества обеспечили существенные преимущества цифровой видеозаписи:

- запись практически не подвержена старению и может храниться сколь угодно долго;
- при копировании не происходит ухудшения качества изображения копий;
- простота выбора любого кадра изображения, его вставки в документ и распечатывания изображения на обычном принтере.

Для регистрации отдельных кадров видеоизображения на бумаге применяются **видеопринтеры**, которые позволяют зафиксировать изображение контролируемой зоны на бумаге.

Провода кабелей электропитания, передачи видеосигналов, управления для исключения возможности их перерезывания или вытягивания помещаются в металлические рукава или трубы.

## 21.3. Средства освещения

Средства освещения включают:

- осветительные приборы;
- устройства управления освещением;
- кабели электропитания.

В качестве осветительных приборов применяются **светильники подвесные** и **консольного типа,** а также **прожекторы**. Светильники наружного освещения закрываются небьющимися колпаками (плафонами) или металлической сеткой. Прожектор представляет собой осветительный прибор дальнего действия, в котором свет концентрируется посредством светооптической системы — металлического зеркала или линзы, в фокусе которых размещается источник света. В зависимости от мощности прожектора диаметр отражателя составляет 25–50 см.

В качестве источников света используются различные **лампы накаливания, газоразрядные лампы** и **ИК-прожекторы**.

**Вакуумные, криптоновые** и **галогенные** лампы накаливания напряжением 220 В выпускаются мощностью до 1000 Вт. Криптоновые лампы содержат нейтральный газ криптон, умень-

шающий испарение вольфрама из раскаленной нити лампы. В галогенной лампе температура нити повышена на 400–500 градусов относительно температуры вакуумных, что увеличивает светоотдачу приблизительно в 1,5 раза. Сохранение более раскаленной вольфрамовой нити от перегорания в течение длительного (в 3–5 раз большего, чем вакуумных) времени эксплуатации достигается в результате так называемого галогенного цикла. С этой целью в колбу лампы вводят йод. Пары йода, взаимодействуя с парами вольфрама, образуют йодистый вольфрам — галоген, который вблизи нити при температуре 2700–2900°С разлагается на йод и вольфрам. Вольфрам оседает на нити и снова испаряется — галогенный цикл повторяется. Так как колба лампы разогревается до температуры 600–700°С, то ее изготавливают из кварцевого стекла. Она имеет меньшие размеры и не боится влаги.

Основной недостаток ламп накаливания — низкая световая отдача (10–26 лм/Вт) и сравнительно малый срок службы (1000–2000 ч).

**Разрядные** лампы имеют световую отдачу в 5–10 раз, а срок службы в 10–20 раз больше. В зависимости от того, что является основным источником излучения, разрядные лампы делятся на следующие группы:

- газо- и паросветные, в которых излучение вызвано возбуждением атомов, молекул или рекомбинацией ионов газов, паров металлов (ртути, натрия) и их соединений;
- люминесцентные, источником света которых являются люминофоры, возбуждаемые излучением разряда;
- электродосветные, в которых свет излучают электроды, раскаленные в разряде до высокой температуры.

**Газоразрядные** лампы широко применяются для освещения улиц и открытых пространств, а люминесцентные лампы — для освещения закрытых помещений (комнат, коридоров). В зависимости от спектра излучения люминофора люминесцентные лампы делятся на лампы дневного света (ЛД) со средней цветовой температурой 6740°К, белого света (ЛБ) — 3500°К, холодного белого света (ЛХБ) — 4300°К и теплого белого света (ЛТБ) — 2700–2800°К. Для сравнения цветовая температура ламп накаливания составляет 2700–2800°К, а солнечного света в полдень — 5400–5800°К. Под

цветовой понимается температура раскаленного тела, спектр излучения которого совпадает со спектром рассматриваемого источника света. Но следует иметь в виду, что люминесцентные лампы создают широкополосные электромагнитные помехи и нуждаются в специальном пускорегулирующем устройстве.

Световой поток от разрядных ламп изменяется с частотой электропитания 50 Гц, что вызывает ухудшение качества изображения при наблюдении с помощью телевизионных камер. При несовпадении частот электропитания лампы и кадровой развертки телевизионной камеры изображение на экране монитора мелькает и изменяются цвета цветного изображения. Хотя в ряде телевизионных камер принимаются меры по устранению этих недостатков, например с помощью электронного затвора, для освещения объектов телевизионного наблюдения используются чаще лампы накаливания.

Для скрытого телевизионного наблюдения за действием злоумышленника применяются также **ИК-осветители**. В качестве источников ИК-света применяют лампы накаливания, закрытые непрозрачными для видимого света фильтрами, и полупроводниковые приборы (светодиоды). Светодиоды по сравнению с лампами имеют меньшие габариты, большую надежность и срок службы (5000 ч), но мощность их излучения мала. Поэтому в ИК прожекторах размещается большое количество светодиодов в виде матриц. Мощность оптического излучения ИК прожекторов составляет 50 Вт при угле рассеянии (10–20)°.

Кабели электропитания осветительных приборов прокладываются, как правило, под землей или в металлических трубах вдоль забора и стен зданий. Допускается использование воздушных сетей электропитания, расположенных на территории таким образом, чтобы исключалась возможность их повреждения, прежде всего, из-за ограждения.

## 21.4. Средства нейтрализации угроз

В качестве звуковых охранных оповещателей применяются электромеханические звонки громкого боя, электромагнитные и пьезоэлектрические сирены с громкостью звука до 120 дБ. В сиренах звук создают колеблющиеся мембрана электромагнита и по-

верхность керамического пьезоэлемента, к которым подводится переменное напряжение от звукового генератора.

В качестве тревожной световой сигнализации могут использоваться источники яркого непрерывного или мигающего света в контролируемой зоне, включаемые автоматически по сигналу тревоги или вручную охраной.

Для ликвидации пожара в любой организации в легкодоступных местах размещаются традиционные **средства пожаротушения**: пенообразующие огнетушители, механические средства (багры, топоры) для разрушения очага пожара, бочки с песком, пожарные рукава и др.

В качестве огнетушащего вещества наиболее широко применяется вода. Но ее нельзя использовать для тушения веществ, которые реагируют с ней, выделяя тепло или горючие, токсичные, коррозионно-активные газы (металлоорганические соединения, карбиды и гидриды металлов и др.). При тушении водой нефти или нефтепродуктов могут произойти выбросы или разбрызгивание горящих продуктов, а электрооборудования — дополнительные очаги горения, вызванные короткими замыканиями воды в нем.

Для улучшения свойств воды как огнетушащего вещества в нее добавляют:

- водорастворимые полимеры для повышения смачиваемости тлеющих материалов;
- полиоксиэтилен для повышения пропускной способности трубопроводов;
- антифризы и соли для уменьшения температуры замерзания.

Применяемая в большом количестве вода для заливания пожара способна нанести значительный ущерб источникам информации и другим материальным ценностям, расположенным вблизи очага горения. Кроме того, горящие нефтепродукты всплывают над водой и недостаточно изолируются от кислорода. Более эффективна **тонкораспыленная вода** с диаметром капель около 100 мкм. Тонко распыленную воду получают в результате подачи ее к распылителю под высоким давлением (до нескольких сот атмосфер), подводкой перегретой воды, воздействием на воду ультразвуковых колебаний от автономного генератора, распылением воды в специальных распылителях сжатым газом азотом.

**Пенное пожаротушение** применяют преимущественно для тушения пожаров в химической и нефтехимической промышленности, в подвалах и отдельных помещениях, в трюмах кораблей. После тушения и прекращения подачи пены по всей поверхности горящего вещества образуется устойчивый пенный слой толщиной до 5 см, который в течение 2–3 часов изолирует горящее вещество от кислорода. Так как пенообразователи представляют собой агрессивные вещества, для их хранения применяют емкости с внутренней поверхностью из нержавеющей стали или полимерных материалов.

**Нейтральные газы** пригодны для тушения пожаров любых классов веществ за исключением склонных к горению без доступа воздуха, самовозгоранию и (или) тлению внутри объема вещества (древесных опилок, хлопка, травяной мука и др.), а также металлов (натрия, калия, магния, титана и др.), гибридных металлов и пирофорных веществ. Так как газы практически не причиняют ущерба в защищаемом объеме, то они все шире применяются для тушения пожара в вычислительных центрах и телефонных узлах, библиотеках, музеях, хранилищах и т. д. Газовые огнетушащие вещества и их составы (смеси) можно условно разделить по способу изготовления на синтезированные (хладоны и элегаз) и натуральные (углекислый газ, азот, аргон, газовые составы инерген и аргонит).

**Синтезированные огнетушащие вещества** обычно более эффективны, чем натуральные, и способны храниться в баллонах в сжиженном состоянии. Но эти газы при высокой температуре (более 600°) частично разрушаются с выделением токсичных коррозионно-активных продуктов пиролиза. Натуральные газовые огнетушащие вещества термически устойчивы, но для хранения в сжиженном состоянии требуется холодильное оборудование.

**Газы**, вытесняя кислород, создают непригодную для дыхания атмосферу. Поэтому газы рекомендуется применять в помещениях, в которых постоянно не присутствуют люди или их количество мало и они могут быстро покинуть помещение. Воздушная среда, содержащая современные газы (хладон 227, хладон 3, «Инерген», перфторбутан) даже при огнетушащей концентрации, пригодна для дыхания во время эвакуации людей из помещения и здания. В настоящее время применение хладонов запрещено ввиду разру-

шения ими озонового слоя Земли. К безопасному и эффективному газу, используемому для пожаротушения пожара закрытых помещений с людьми, относится перфторбутан. Он не разрушает озоновый слой, не токсичен, не оставляет следы при применении.

**Порошковое пожаротушение** применяется для тушения пожаров класса A, B, C и D, в том числе при тушении проливов горючих жидкостей или утечке газов из установок, расположенных на открытом воздухе. Огнетушащий порошок содержится в кассете (модуле), из которого он выталкивается пиротехническим составом при его взрыве. В результате образуется облако порошка, движущееся в заданном телесном угле (зоне) с большой скоростью, которое кроме обычного огнетушащего действия эффективно сбивает пламя горения. В качестве огнетушащего порошка применяют бикарбонат натрия (ПСБ-3М), аммофос (П2-АШ), фосфаты и сульфаты аммония (ПИРАНТ-А) и др. Огнетушащие порошки можно хранить и применять при температуре до минус 50°С, они нетоксичны, малоагрессивны, сравнительно дешевы и удобны в обращении. Но порошок при долгом хранении слеживается (твердеет), что требует периодической перезарядки устройств порошкового пожаротушения. Кроме того, при их применении в помещении происходит полная потеря видимости и затрудненное дыхание. Поэтому перед их применением необходима эвакуация персонала из зоны тушения, а после тушения трудоемкая работа по уборке помещения и удаления порошка.

**Огнетушащие аэрозоли** образуются при горении аэрозолеобразующего состава (АОС) и используются сравнительно недавно. Аэрозоль содержит твердые частицы огнетушащего порошка размером 1–10 мкм и подается на значительные расстояния струей углекислого газа, азота и др., образующейся при горении АОС. Мелкодисперсионный аэрозоль создает обширную поверхность, покрывающую очаг пожара, и может находиться длительное время (до 30 минут) во взвешенном состоянии, что обуславливает их высокую огнетушащую способность. Аэрозоль не оказывает вредного воздействия на одежду и тело человека, а также не приводит к коррозии большинство электроизоляционных материалов. Но при применении аэрозолей создается повышенная температура и давление газовой смеси, а в защищаемом помещении резко ухудшает-

ся видимость. Поэтому до применения аэрозольного тушения пожара помещения должны быть покинуты людьми. Кроме того, аэрозольное тушение не применяется во взрывопожароопасных помещениях, в помещениях с легко воспламеняемыми материалами, веществами или предметами. Больше преимуществ имеют так называемые «холодные» аэрозоли, имеющие меньшие размеры высокотемпературной зоны или не имеющие ее вовсе.

Классификация установок пожаротушения, использующих рассмотренные огнетушащие вещества, приведена на рис. 21.2.


*Рис. 21.2.* Классификация средств пожаротушения

Автоматические установки пожаротушения автоматически обнаруживают загорание, подают огнетушащее вещество и оповещают персонал или дежурную смену о пожаре. В автоматизированных установках решение о включении установки пожаротушения производится вручную.

Автоматические установки водяного и пенного пожаротушения делятся на:

- спринклерные, осуществляющие тушение на площади горения;
- дренчерные, обеспечивающие тушение одновременно по всей площади помещения.

**Дренчерные** установки имеют автоматический, дистанционный и ручной пуск, спринклерные — только автоматический пуск. В **спринклерной** установке при возникновении горения в помеще-

нии от температуры вскрывается легкоплавкий замок спринклера (оросителя), и огнетушащее вещество по трубопроводу через ороситель подается в очаг пожара. При этом включаются оповещатели пожара и насосы, непрерывно обеспечивающие подачу тушащего вещества. Если используется дренчерная установка, то при возникновении пожара в помещении срабатывает извещатель, который по шлейфу подает сигнал тревоги, включающий оповещатели и насосы, подающие по трубопроводам огнетушащее вещество на все распылители помещения.

**Современные системы автоматического газового пожаротушения** обеспечивают тушение пожара путем заполнения помещения с очагом возгорания газом по сигналу «Пожар» от извещателей, установленных в этом помещении. Типовой комплекс содержит:

- модуль газового пожаротушения с баллонами газа объемом 40–100 л, запорно-пусковым устройством, манометром и пиропатроном, размещаемыми в специальном помещении (станции газового пожаротушения);
- пожарные (пожарно-охранные) извещатели и шлейфы;
- приемно-контрольный прибор, к входным клеммам которого подключаются шлейфы от извещателей, а с выходных клемм снимаются сигналы управления подрывом пиропатрона, отключения вентиляции, включения табло оповещения сотрудников о подаче газа;
- газопроводы (трубы) от газовой станции к помещениям и газовые распылители в помещениях;
- кнопки ручного пуска и его блокировки.

Через ПКП комплекса газового пожаротушения сопрягается с ПКП автономной системы охраны и с пультом наблюдения централизованной системы.

Инерционность средства пожаротушения в секундах оценивается по времени выхода его на рабочий режим с момента обнаружения пожара. Чем она меньше, тем эффективнее средство пожаротушения. Ориентировочные значения инерционности разных установок составляют:

- спринклерные водозаполненные — 5 мин;
- спринклерные сухотрубные — 8 мин;

- дренчерные с электропуском — 3 мин;
- дренчерные с пневмопуском — 6 мин;
- газовые — 15 с;
- аэрозольные — 5 с.

При выборе установок пожаротушения также учитываются их экономические показатели — затраты на защиту 1 м$^3$ объема и 1 м$^2$ площади. Наименьшие удельные затраты без учета затрат на приобретение технических средств требуются при применении аэрозольных установок, немного дороже спринклерные и дренчерные установки водяного и пенного пожаротушения, далее — порошковые установки, газовые установки. Самые дорогие — модульные установки с токораспыленной водой.

**Резервное или аварийное электропитание** включается автоматически или дежурным (оператором, охранником) при отключении по тем или иным причинам (неисправности или действий злоумышленника) основного электропитания 220 В 50 Гц. Очевидно, что обеспечить резервное электропитание в полном объеме, особенно для крупных систем охраны, сложно и дорого. Поэтому на резервное электропитание переключают в основном средства управления, извещатели и аварийное освещение, которое составляет небольшую часть (около 5% по мощности) от дежурного освещения.

В качестве источников резервного электропитания систем охраны применяются гальванические батареи и аккумуляторы. Только на важных объектах с непрерывным функционированием (в крупных больницах и госпиталях, на атомных электростанциях, в центрах управления и др.) в качестве аварийного электропитания используются автоматически включаемые мощные дизель-генераторы, часть энергии которых отводится для системы охраны. В таких организациях доля элементов системы охраны, подключаемых к резервному питанию, может быть выше.

Батареи с напряжением питания 12 и 24 В создаются на базе угольно-цинковых, щелочных и ртутных гальванических элементов. Наиболее дешевыми являются угольно-цинковые элементы, но они имеют невысокую удельную мощность (5–10 Вт/кг), значительное снижение напряжения при разряде и малый срок хранения. Номинальное напряжение элемента составляет 1,5 В. Щелочные

элементы отличаются от угольно-цинковых щелочным электролитом, имеют более высокую удельную мощность (100–150 Вт/кг) и более длительный срок хранения. Напряжение щелочного элемента равно 1,4 В. В ртутных элементах в качестве анода используется оксид ртути, а катод выполняется из смеси порошка цинка и ртути. Анод и катод разделены сепаратором, пропитанным 40% раствором щелочи. Ртутные элементы отличаются высокой удельной энергией (90–120 Втч/кг), стабильностью напряжения и высокой механической прочностью. Напряжение ртутного элемента около 1,25 В.

Батареи имеют сравнительно небольшую емкость (максимум — единицы Ач) и применяются для резервного электропитания слаботочных потребителей, в основном извещателей.

Аккумуляторы являются химическими источниками электрической энергии многоразового действия. Они состоят из двух электродов (положительного и отрицательного), электролита и корпуса. Накопление энергии в аккумуляторе происходит при его зарядке от внешнего источника тока (зарядного устройства, подключенного к сети) в результате химической реакции окисления-восстановления электродов. При разряде аккумулятора происходят обратные процессы. Для получения напряжения питания 12 и 24 В отдельные аккумуляторы (элементы, банки) последовательно соединяются в батареи. Характеристики распространенных типов аккумуляторов приведены в табл. 21.2.

*Таблица 21.2*

| *Тип элемента* | *Рабочее напряжение, В* | *Максимальная емкость, Ач* | *Относительная стоимость одного Втч энергии* |
|---|---|---|---|
| Свинцово-кислотный | 2,0 | 55 | 1 |
| Железо-никелевый | 1,2 | 195 | 3 |
| Никель-кадмиевый | 1,2 | 165 | 2 |
| Серебряно-кадмиевый | 1,05 | 230 | — |
| Серебряно-цинковый | 1,5 | 285 | 15 |

Широко распространенные кислотные аккумуляторы, выполненные по классической технологии, дешевы, но требуют дополни-

тельных затрат на их обслуживание, специальных (с хорошей вентиляцией воздуха) помещений и обученного персонала. Наиболее удобными и безопасными из кислотных аккумуляторов являются необслуживаемые герметичные аккумуляторы, произведенные по технологии «dryfit». Электролит в этих аккумуляторах находится в желеобразном состоянии, что существенно повышает надежность аккумуляторов и безопасность их эксплуатации.

### Вопросы для самопроверки

1. Классификация извещателей по назначению, принципам работы и виду зоны обнаружения.
2. Типы контактных извещателей, принципы работы магнитоконтактных извещателей.
3. Типы акустических извещателей. Способы повышения помехоустойчивости ультразвуковых извещателей.
4. Типы оптико-электронных извещателей. Принципы повышения помехоустойчивости пассивных и активных оптико-электронных извещателей.
5. Типы микроволновых радиоизвещателей. Принципы повышения помехоустойчивости объемных радиолучевых извещателей.
6. Типы и принципы работы вибрационных извещателей.
7. Принципы пожарных извещателей.
8. Преимущества и недостатки тепловых извещателей.
9. Функции приемно-контрольных приборов и пультов централизованной охраны.
10. Типы средств передачи извещений.
11. Классификация телевизионных камер по функциям и конструкции.
12. Виды мониторов. Преимущества и недостатки мониторов на панелях.
13. Средства, применяемые для обработки видеосигналов. Принципы работы детектора движения.
14. Средства, применяемые для уменьшения количества мониторов на рабочем месте сотрудника охраны.

15. Средства, применяемые для записи видеосигналов. Принципы повышения времени записи на одну кассету.
16. Типы средств освещения. Особенности галогенных ламп накаливания.
17. Средства, применяемые для нейтрализации угроз. Типы установок пожаротушения.
18. Виды средств аварийного электропитания. Типы химических элементов электропитания.

# Глава 22. Средства противодействия наблюдению

## 22.1. Средства противодействия наблюдению в оптическом диапазоне

Основными средствами скрытия объектов наблюдения в оптическом диапазоне являются краски, различные маски и экраны. При выборе красок для маскировочного окрашивания кроме цвета важно учитывать характер изменения коэффициента отражения от длины волны. Чем меньше отличаются коэффициенты отражения краски в видимом и инфракрасном диапазонах волн, тем лучше ее маскирующая способность.

Искусственные оптические маскировочные маски в зависимости от ее формы и способа расположения возле объекта делятся на следующие типы:

- маски-навесы;
- вертикальные маски;
- маски перекрытия;
- наклонные маски;
- радиопрозрачные маски.

**Маски-навесы** предназначены для скрытия объектов, расположенных на открытых сверху площадках и защищают их от наблюдения с помощью средств, размещаемых на верхних этажах высотных зданий, возвышенностях и горах, на самолетах и космических аппаратах.

**Вертикальные маски** защищают объекты от наблюдения с земли. Маски перекрытия состоят из каркаса и маскировочного покрытия, которые полностью закрывают объект. Они применяются, прежде всего, для защиты объектов, перевозимых на открытых платформах.

**Наклонные маски** используются в основном для скрытия теней объемных объектов, по длине которых с учетом положения солнца определяют высоту объектов при наблюдении сверху (с самолетов и космических аппаратов).

**Радиопрозрачные маски** выполняются из радиопрозрачных материалов (стеклопластика, пенопласта и др.), обычно в форме

шара, для скрытия демаскирующих признаков и физической защиты антенн.

**Искусственные оптические маски** изготовляются из подручных материалов (хвороста, камыша, тростника, кустарника) или из табельных средств и материалов (маскировочной сети, устойчивой к воздействию факторов погоды, армированной маскировочной бумаги, сетчатой ткани, полихлорвиниловой пленки и др.), а также в виде различных сборных возимых маскировочных комплектов.

Для маскировки военной техники в оптическом диапазоне используются различные типы **табельных маскировочных комплектов (МКТ)**: МКТ-Л — для маскировки на растительном фоне или обнаженном грунте, МКТ-С — для снежных фонов, МКТ-П — для горно-пустынной местности, МКТ-Т — для маскировки танков и др. Комплект представляет собой металлический разборный каркас, на который натягивается окрашенная в различные цвета специальная сплошная или сетчатая ткань с двусторонней окраской для разных фонов. Маскировочное покрытие одного комплекта имеет максимальный размер 12 × 18 м (из расчета создания маски для танка) и состоит из 12 фрагментов размером 3 × 6 м каждый. Фрагменты соединяются между собой сшивными шнурами, которые позволяют оперативно собирать покрытия различной конфигурации и размера, в том числе плоские, выпуклые, вертикальные, наклонные, маски-макеты, маски-навесы. С помощью запасных сшивных шнуров, входящих в маскировочный комплект, можно объединять покрытия несколько комплектов для укрытия крупных объектов.

Искусственные оптические маски могут применяться многократно, не оказывают вредное воздействие на природу, совместимы с другими способами защиты.

**Светонепроницаемые одно- и многоцветные воздушные пены**, быстро наносимые с помощью генераторов пены на объекты, обеспечивают их эффективную маскировку в широком диапазоне длин волн в течение до нескольких часов.

Маски, которые создают у наблюдателя представление о другом объекте (объекте прикрытия), называются **деформирующими**. Например, при перевозке орудий на железнодорожных платформах их скрывают под брезентом, которым накрывают деревянный пря-

моугольный каркас. Наблюдатель по факту присутствия часовых на платформе сделает вывод о перевозке военной техники, но определить вид перевозимой техники не сможет. Во время битвы за Москву с помощью деформирующих масок и имитационного окрашивания для дезинформирования немецких летчиков мавзолей Ленина имел сверху вид двухэтажного особняка, а кремлевские башни были похожи на водонапорные башни и высотные здания.

Для дезинформирующего скрытия применяются кроме деформирующих масок **ложные сооружения** и **конструкции**, создающие признаки ложного объекта (объекта прикрытия). Ложные сооружения могут быть плоскими и объемными, функциональными и нефункциональными. Они относятся к наиболее дорогим средствам защиты информации, особенно объемные и функциональные, так как должны воспроизводить полный набор демаскирующих признаков объекта прикрытия в динамике в течение всего периода защиты. Если, например, имитируется объект, на котором работают люди, то они должны убедительно изображать соответствующую деятельность, а не устраивать непрерывные перекуры или греться на солнышке.

Энергетическое скрытие демаскирующих признаков объектов достигается путем уменьшения яркости объекта и фона ниже чувствительности глаза или технического фотоприемника, а также их ослепления. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Для экранирования объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки. Эффективные экраны создают жалюзи. По виду материалов жалюзи делятся на тканевые, пластиковые, деревянные и металлические. Лучшие эксплуатационные свойства имеют деревянные и металлические жалюзи. По расположению ламелей жалюзи бывают вертикальные, горизонтальные и рулонные.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают рассмотренные искусственные маски, а также естественные и искусственные аэрозоли в среде распространения.

**Аэрозоли** — вещества в виде дисперсии твердых частиц и капель жидкости, находящихся во взвешенном состоянии в воздухе. К аэрозолям относятся обычно дымы, туманы, пыль, смог.

Естественные аэрозоли образуются обычно пылью и частицами воды. В зависимости от размеров частиц воды метеорологическая дальность изменяется от десятков метров (при очень сильном тумане, дожде и снеге) до 10–20 км (при дымке). Хорошая видимость обеспечивается при дальности 20–50 км, а исключительно хорошая — более 50 км.

Наиболее распространенной разновидностью аэрозольного состояния атмосферы является дымка. Дымка возникает при слипании мелкодисперсных частиц воздуха друг с другом и взаимодействии их с атмосферной влагой. В условиях повышенной влажности воздуха в результате взаимодействия паров воды с частицами растворимых в ней солей образуется туманная дымка, при которой метеорологическая дальность составляет 1–10 км.

Влияние аэрозольных образований в общем случае проявляется как в рассеянии, так и поглощении света частицами аэрозоля. Коэффициент ослабления (поглощения) в видимой области спектра изменяется в 1,5–2 раза. С увеличением длины волны потери ослабевают. Потери энергии волны при $\lambda = 0{,}55$ мкм приблизительно в 10 раз больше потерь для $\lambda = 1{,}06$ мкм. Аэрозольное рассеяние света зависит от коэффициентов его ослабления отдельными частицами, их концентрации и размеров. Оно определяет прозрачность и метеорологическую дальность видимости.

Использование естественных аэрозолей в качестве средств защиты от наблюдения затруднено из-за случайного характера их проявлений в виде образований, приводящих к малой метеорологической дальности. Тем не менее естественные аэрозоли в виде облаков создают серьезные проблемы для разведки при наблюдении наземных и надводных объектов с помощью средств космической разведки. Учитывая, что траектории движения КА и облаков независимые, вероятность выполнения временного условия разведывательного контакта (совпадения моментов пролета спутника над интересующим разведку объектом и отсутствием облачности) равна произведению вероятностей каждого из этих событий. Следовательно, для обнаружения и распознавания объекта

даже при отсутствии мер защиты информации о нем потребуются многократные пролеты над ним разведывательных КА.

С помощью дымовых шашек, специальных боеприпасов (снарядов, бомб), аэрозольных генераторов и дымовых машин создаются дымовые завесы (облака) из искусственных аэрозолей, обеспечивающих (при учете направления и силы ветра) эффективное, но кратковременное скрытие. Время и площадь скрытия зависят от многих факторов, в том числе от объема облака дыма, направления и скорости ветра, и колеблется от минут до 1–2 часов. Наиболее эффективные завесы образуются при скорости ветра 3–5 м/с.

В качестве химических веществ для образования дыма применяются эпоксидные, фенольные, полиэтиленовые, силикатные, уретановые смолы и другие высокомолекулярные соединения. Дымы из таких веществ получаются разделением частиц вещества в потоке горячих газов и другими способами. В зависимости от состава компонентов частицы, образующие аэрозольное облако, могут иметь диаметр от 1 до 100 мкм. Для образования аэрозольного облака, обеспечивающего, например, ослабление излучений в ИК-диапазоне примерно в 80 раз, на площади 600 м$^2$ потребуется распылить около 400 г дымообразующего вещества [11].

Кроме того, на яркость объекта с собственными источниками тепла, и, следовательно, на его контраст с фоном в ИК-диапазоне влияет температура поверхности объекта. Для защиты объектов от наблюдения в инфракрасном диапазоне применяются различные теплоизолирующие экраны, в том числе подручные материалы с плохой теплопроводностью: листья деревьев и кустарников, сено, брезент и др. Хорошими теплоизолирующими свойствами обладают воздушные пены.

Так как скрытое наблюдение проводится, как правило, с помощью оптических приборов, то для противодействия наблюдению применяются активные средства обнаружения оптики. Такие средства представляют собой приборы ночного видения с лазерной подсветкой. Средство содержит лазерный излучатель в инфракрасном диапазоне длин волн, лучи которого сканируют наблюдаемое пространство. Отраженный от поверхности линзы объектива луч лазера обозначает место нахождения оптического прибора точкой повышенной яркости на изображении.

## 22.2. Средства противодействия радиолокационному и гидроакустическому наблюдению

Для структурного скрытия объектов радиолокационного наблюдения применяются конструкции, переотражающие падающие на них электромагнитные волны радиолокатора в обратном направлении и создающие на экране локатора ложные «блестящие» точки. Так как точно направление на радиолокатор объекту защиты неизвестно, то такие конструкции должны создавать «блестящие точки» в достаточно широком угле возможных направлений. В качестве таких широкоугольных конструкций используются уголковые, линзовые, дипольные отражатели и переизлучающие антенные решетки (ПАР).

**Уголковый радиоотражатель** состоит из жестко связанных между собой взаимно перпендикулярных плоскостей (см. рис. 22.1).

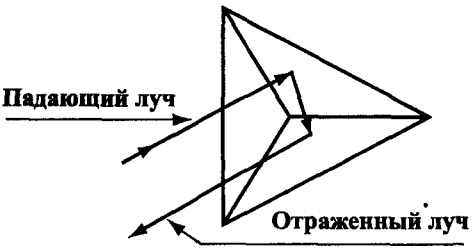



*Рис. 22.1.* Схема уголкового отражателя

Важнейшим свойством уголковых отражателей является то, что значительная доля энергии волны, падающей на них с любого направления в пределах достаточно большого угла (около 80 градусов), отражается обратно в сторону облучающей РЛС. Благодаря этому уголковые радиоотражатели даже небольших размеров имеют значительную эффективную площадь рассеяния. Например, ЭПР трехгранного уголкового отражателя с размерами граней 0,5 м и длиной волны РЛС 3 см составляет 290 м$^2$, в то время как ЭПР самолета-бомбардировщика В-52 с длиной фюзеляжа и размахом крыльев в десятки метров составляет около 100 м$^2$ [11].

**Линзовые отражатели** создаются на основе линз Люнеберга. Линза представляет собой многослойный шар с различными значениями диэлектрической проницаемости слоев (рис. 22.2).

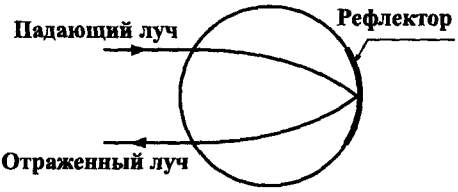



*Рис. 22.2.* Схема линзы Люнеберга

При такой конструкции электромагнитные волны фокусируются на внутренней поверхности шара, покрытой металлической радиоотражательной пленкой-экраном. Ширина диаграммы рассеяния линзы зависит от размеров экранирующей поверхности сферы и достигает 140 градусов. ЭПР линзового отражателя диаметром 60 см и массой 40 кг достигает на длине волны $\lambda = 10$ см величины более 150 м$^2$, на $\lambda = 3$ см более 1800 м$^2$ [11].

Переизлучающие антенные решетки (ПАР) состоят из набора обычных антенн, которые работают в режиме переизлучения принимаемых сигналов. Такой режим достигается путем замыкания антенн в точке подключения фидера или волновода. Простейшие ПАР образуются при попарном соединении элементарных полуволновых вибраторов.

Уголковые радиоотражатели, линзы Люнеберга, ПАР, размещенные вблизи защищаемого объекта, создают на экране РЛС многочисленные яркие засветки, среди которых трудно обнаружить маскируемый объект.

Для маскировки воздушных объектов применяют **дипольные радиоотражатели (диполи)**. Они представляют собой полоски металлизированной бумаги или алюминиевой фольги, металлизированные стеклянные или нейлоновые волокна, разбрасываемые в зоне расположения защищаемого объекта. Длина диполей и их толщина выбираются так, чтобы обеспечить эффективное рассеивание радиоволн по возможности в более широком диапазоне частот. Диполи в виде металлизированных стекловолокон имеют длину 35–40 см и толщину 0,025 мм, медная проволока толщиной в доли

мм нарезается длиной около 50 см. Дипольные отражатели обычно упаковываются в пачки из десятков и сотен тысяч штук и при выбрасывании с самолета в воздух создают облако медленно опускающихся на землю отражателей. Отраженные от них сигналы наблюдаются на экране индикатора РЛС в виде множества ярких точек, маскирующих отраженный от самолета сигнал. Если последовательно сбрасывать достаточно большое количество пачек, то на экране РЛС образуются засвеченные полосы, в которых трудно обнаруживать воздушные объекты.

Энергетическое скрытие достигается за счет уменьшения эффективной площади рассеяния объекта в основном двумя способами: изменением диаграммы направленности отражающей поверхности объекта и поглощением облучающей энергии РЛС. Уменьшение отраженной энергии для объекта, подлежащего защите от радиолокационного наблюдения, должно предусматриваться еще при его создании путем исключения на поверхности объекта плоскостей, образующих уголковые отражатели. ЭПР конусообразных и шарообразных форм в сотни раз меньше уголковых отражателей. Готовые изделия, имеющие поверхности сложной формы с резкими переходами, целесообразно накрывать экранами, искажающими и отклоняющими диаграмму направленности объектов, лучше всего шарообразной формы.

Для энергетического скрытия объектов от радиолокационного наблюдения его поверхность покрывают материалами, обеспечивающими градиентное и интерференционное поглощение облучающей электромагнитной энергии.

**Градиентное поглощение** обеспечивают многослойные материалы, каждый слой которых состоит из основы — диэлектрика (стеклотекстолита, пенопласта, каучука и др.) и наполнителя (ферритов, карбонильного железа, порошка графита, угольной пыли и др.), поглощающего электромагнитную энергию. Внешний слой поглотителя имеет диэлектрическую проницательность, близкую к 1, а для увеличения поверхности имеет рифленую структуру или шипы. В каждом последующем слое диэлектрическая проницаемость увеличивается. По мере проникновения электромагнитной волны в поглощающий материал ее энергия убывает, а направление изменяется. В результате искривления направления распро-

странения волны удлиняется ее путь в поглощающем материале и, следовательно, увеличивается поглощение. Например, покрытие из пористого стекловолокна толщиной 12,7 мм поглощает до 99% энергии электромагнитной поля в см-диапазоне длин волн [11].

Другой вид радиопоглощающего материала — **интерференционный** обеспечивает интерференцию прямой (падающей) и отраженной от объекта электромагнитных волн. Простейший поглощающий материал этого вида состоит из слоя диэлектрика и электропроводящей пленки. Тип и толщина диэлектрика, магнитная проницаемость и волновое сопротивление пленки выбираются такими, чтобы сдвиг по фазе между падающей и отраженной волнами был близок к 180°. В результате наложения прямой и отраженной волн в диэлектрике возникают стоячие волны и происходит подавление падающей волны отраженной волной. В результате этого ЭПР объекта резко уменьшается. Однако такой эффект наблюдается в узком диапазоне длин волн. Для расширения диапазона применяются многослойные материалы, каждый слой которых рассчитан на свой диапазон длин волн облучающей электромагнитной волны. Но многослойные материалы, обеспечивающие эффективное поглощение в достаточно широком диапазоне частот, толстые и тяжелые.

В современных поглощающих материалах используют оба способа уменьшения энергии отраженной электромагнитной волны. Например, коэффициент отражения керамического ферритового радиопоглощающего материала составляет 10% в диапазоне волн 30–300 МГц при толщине ферритового слоя 0,83 см. Созданы достаточно легкие радиопоглощающие материалы в виде многослойной ткани.

Примером технических решений, обеспечивающих эффективное структурное и энергетическое скрытие, является технология снижения ЭПС «Стелс». Она предусматривает:

- совершенствование формы объекта защиты путем уменьшения площадей его поверхностей, исключения углов их облучения близких 90°, замены прямых плоскостей кривыми, устранения резонансных явлений на облучаемой поверхности;
- применение неметаллических композиционных материалов, слабо рассеивающих энергию электромагнитного поля радиолокационной станции;

- использование высокоэффективных (с большим коэффициентом поглощения и малым весом) материалов, поглощающих и рассеивающих электромагнитную волну.

В результате использования этой технологии эффективная площадь рассеяния (ЭПР) самолетов-бомбардировщиков В-1 и В-2 существенно снижена по сравнению с бомбардировщиком В-52 — с 100 м$^2$ до единиц м$^2$. Кроме авиации эта технология внедряется при строительстве надводных боевых кораблей.

Другой способ энергетического скрытия, который широко применяется для защиты объектов от радиолокационного наблюдения, — **генерация помех**. Простейшей помехой является гармоническое колебание на частоте РЛС, создаваемое генератором помех в месте нахождения защищаемого объекта. Так как диаграмма направленности антенны РЛС имеет, как правило, боковые лепестки, то такая помеха создает шумовую засветку экрана локатора.

Более сложной по структуре является модулированная помеха с одним или несколькими изменяющимися параметрами. Модулированная помеха бывает непрерывной и импульсной и обладает спектром, близким к спектру излучения РЛС. По эффекту воздействия помехи классифицируются на маскирующие изображение объекта путем зашумления экрана РЛС и имитирующие на нем ложные световые пятна. Изменяя структуру и время задержки имитационной помехи, можно менять форму, место и характер движения ложной засветки на экране локатора.

Защита информации об объектах, находящихся в воде, предусматривает, прежде всего, защиту от гидроакустического наблюдения. Способы этой защиты по сути соответствуют рассмотренным с учетом особенностей канала утечки. В качестве основных применяются следующие:

- маскировка с использованием природных явлений. При перепаде температуры слоев возникают акустические экраны, труднопреодолимые для акустических излучений;
- использование звукопоглощающих покрытий сотовой конструкции из нейлона, полиэтилена, полипропилена и различных пластмасс, а также содержащих натуральный каучук. За рубежом проводятся опыты по покрытию корпусов подводных лодок материалами, поглощающими до 90% акустической энергии;

- создание активных помех гидролокаторам, в том числе путем ретрансляции облучающих сигналов с усилением их мощности.

**Вопросы для самопроверки**

1. Типы искусственных оптических масок.
2. Особенности применения аэрозолей как средств энергетического скрытия.
3. Средства, используемые для скрытия объектов радиолокационного наблюдения.
4. Материалы, применяемые для электромагнитного поглощения.
5. За счет чего достигается в технологии «Стелс» существенное снижение эффективной площади рассеяния объектов?

# Глава 23. Средства противодействия подслушиванию

## 23.1. Средства звукоизоляции и звукопоглощения акустического сигнала

Звукоизоляция обеспечивается с помощью архитектурных и инженерных конструкций: звукоизолирующих ограждений помещений и зданий, экранов, кабин, кожухов (рис. 23.1).


*Рис. 23.1.* Основные средства звукоизоляции

**Звукоизолирующие ограждения** помещений и зданий — это стены, перекрытия, перегородки, окна, двери, имеющие по периметру контакты с другими ограждениями. Величина звукоизоляции однослойного ограждения характеризуется сложной нелинейной зависимостью как от частоты $f_{зв}$ колебания акустической волны, так и от большой группы характеристик ограждения. В общем случае эту зависимость можно представить в виде следующей функции:

$$R = F(f_{зв}, m, h/f_{ог}, \rho, v),$$

где m — поверхностная масса (масса 1 м$^2$) ограждения; h — коэффициент потерь энергии в материале; $f_{ог}$ — собственная частота колебаний ограждения; ρ — удельная плотность материала ограждения; v — скорость звука в материале ограждения.

Звукоизоляция ограждающей конструкции, содержащей несколько элементов, должна оцениваться звукоизоляцией наиболее слабого элемента. Такими элементами чаще бывают **однослойные плоские ограждения**. Для повышения величины ослабления

на плоское ограждение наносят слой звукопоглощающего материала, которое увеличивает звукоизоляцию R за счет дополнительного ослабления звука в звукопоглощающем материале и повышения общей массы составного ограждения.

Для повышения звукоизоляции применяют также **многослойные ограждения**, чаще двойные. Они состоят из двух однослойных поверхностей, разделенных в простейшем случае воздушным слоем. Между поверхностями, соединенными ребрами жесткости, помещают различные звукопоглощающие материалы.

Значения ослабления звука ограждениями (стенами и межэтажными перекрытиями), выполненными из некоторых часто применяемых строительных конструкций, указаны в табл. 23.1 и 23.2.

*Таблица 23.1*

| *Вид стены* | *Толщина, мм* | *Звукоизоляция в дБ на частотах в Гц* | | | | |
|---|---|---|---|---|---|---|
| | | *250* | *500* | *1000* | *2000* | *4000* |
| Кирпичная кладка, оштукатуренная с двух сторон | 0,5 кирпича | 40 | 42 | 48 | 54 | 60 |
| | 1 кирпич | 44 | 51 | 58 | 64 | 65 |
| | 1,5 кирпича | 48 | 55 | 61 | 61 | 65 |
| | 2 кирпича | 52 | 59 | 65 | 70 | 70 |
| | 2,5 кирпича | 55 | 60 | 67 | 70 | 70 |
| Железобетонные панели | 100 | 40 | 44 | 50 | 55 | 60 |
| | 200 | 47 | 51 | 60 | 63 | 65 |
| | 300 | 50 | 58 | 65 | 65 | 65 |
| | 400 | 55 | 61 | 68 | 70 | 70 |
| Керамзитовая панель | 80 | 34 | 39 | 47 | 52 | 60 |
| | 120 | 37 | 39 | 47 | 54 | 51 |
| | 140 | 43 | 47 | 53 | 57 | 61 |
| Гипсобетонная панель | 86 | 33 | 39 | 47 | 54 | 60 |
| Шлакоблоки, оштукатуренные с двух сторон | 220 | 42 | 48 | 54 | 60 | 63 |
| Древесностружечная плита | 30 | 26 | 26 | 26 | 26 | 26 |

*Таблица 23.2*

| *Вид межэтажного перекрытия* | *Толщина перекрытия, мм* | *Звукоизоляция в дБ на частотах в Гц* | | | | |
|---|---|---|---|---|---|---|
| | | *250* | *500* | *1000* | *2000* | *4000* |
| Железобетонная панель | 120 | 45 | 51 | 58 | 58 | 58 |
| Железобетонная панель | 160 | 47 | 52 | 56 | 61 | 61 |
| Железобетонная плита с круглыми пустотами | 160 | 38 | 47 | 53 | 57 | 57 |
| Железобетонная плита с овальными пустотами и бетонной стяжкой | 220 | 49 | 55 | 59 | 62 | 66 |

Одними из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются **двери** и **окна**. Двери имеют существенно меньшие по сравнению с основными ограждающими конструкциями поверхностные плотности, а также зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации в помещениях от подслушивания. Повышение звукоизоляции дверей обеспечивается:

- устранением щелей между дверью и дверной коробкой путем применения уплотняющих прокладок из резины, порога или резинового фартука между дверью и полом;
- применением для дверного полотна более плотных пород дерева, увеличением толщины дверного полотна и обивки его дерматином или аналогичным материалом по слою войлока или ваты с валиком по периметру двери;
- установкой звукоизолирующей двери, выполненной в виде многослойного дверного полотна с размещением между слоями звукоизолирующего материала;
- установкой двойных дверей с тамбуром между ними шириной 20–30 см.

В табл. 23.3 приведены примеры повышения звукоизоляции дверей путем применения дополнительных уплотняющих прокладок по периметру притвора дверей.

*Таблица 23.3*

| *Конструкция двери* | *Условия применения* | *Звукоизоляция в дБ на частотах, в Гц* | | | | |
|---|---|---|---|---|---|---|
| | | *250* | *500* | *1000* | *2000* | *4000* |
| Стандартное дверное полотно толщиной 40 мм | без уплотняющих прокладок | 14 | 16 | 22 | 22 | 20 |
| | с прокладками из пористой резины | 16 | 25 | 26 | 26 | 23 |
| Щитовая дверь толщиной 40 мм, обшитая фанерой с двух сторон | без уплотняющих прокладок | 23 | 24 | 24 | 24 | 23 |
| | с прокладками из пористой резины | 27 | 32 | 35 | 34 | 35 |
| Щитовая дверь из древесноволокнистых плит толщиной 4–6 мм с воздушным зазором 50 мм | без уплотняющих прокладок | 26 | 30 | 31 | 28 | 29 |
| | с прокладками из пористой резины | 30 | 33 | 36 | 32 | 30 |
| Дверь звукоизолирующая облегченная, с прокладками из пористой резины | | 30 | 39 | 42 | 45 | 42 |
| Дверь звукоизолирующая облегченная, двойная с тамбуром шириной 200 мм, с прокладками из пористой резины | | 42 | 55 | 58 | 60 | 60 |
| Дверь звукоизолирующая тяжелая, с прокладками из пористой резины | | 36 | 45 | 51 | 50 | 49 |
| Дверь звукоизолирующая тяжелая, двойная с тамбуром шириной 300 мм, с прокладками из пористой резины | | 46 | 60 | 60 | 65 | 65 |
| Дверь звукоизолирующая тяжелая, двойная с тамбуром шириной 300 мм с облицовкой тамбура звукопоглощающими материалами, с прокладками из пористой резины | | 58 | 65 | 70 | 70 | 70 |

Уплотнение притворов повышает звукоизоляцию дверей на 5–10 дБ. Однако необходимо учитывать, что в процессе эксплуатации в результате обжатия, износа, затвердевания резиновых прокладок

звукоизоляция снижается. Дополнительные меры повышают звукоизоляцию дверей на 10–15 дБ, а применение тамбуров увеличивает ее примерно на 20 дБ.

Следовательно, для защиты информации необходимо применять либо специально разработанные звукоизолирующие двери, либо двойные двери с тамбуром. При этом целесообразно применять утяжеленные полотна дверей, обивать их материалами со слоями ваты или войлока, использовать дополнительные уплотнительные прокладки, герметизирующие наплавы, валики и т. п. При организации тамбуров дверей звукоизоляцию повышает уплотнение щелей над полом при отсутствии порогов, а также полезна облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями.

Окна, занимающие для обеспечения освещенности достаточно большие площади ограждающих конструкций помещений, часто являются, так же как и двери, элементом среды распространения потенциальных каналов утечки информации. Значения звукоизоляции окон различных схем остекления приведены в табл. 23.4.

*Таблица 23.4*

| *Схема остекления* | *Звукоизоляция в дБ на частотах Гц* | | | | |
|---|---|---|---|---|---|
| | *250* | *500* | *1000* | *2000* | *4000* |
| *1* | *2* | *3* | *4* | *5* | *6* |
| Одинарное остекление, мм: | | | | | |
| 3 | 17 | 22 | 28 | 31 | 32 |
| 4 | 23 | 26 | 31 | 32 | 32 |
| 6 | 22 | 26 | 30 | 27 | 25 |
| Двойное остекление с воздушным промежутком, мм: | | | | | |
| 3–57–3 | 20 | 32 | 41 | 49 | 46 |
| 3–90–3 | 29 | 38 | 44 | 50 | 48 |
| 4–57–4 | 31 | 38 | 46 | 49 | 55 |
| 4–100–4 | 35 | 39 | 47 | 49 | 52 |
| 4–200–4 | 36 | 41 | 47 | 49 | 55 |
| Тройное остекление с двумя воздушными промежутками*), мм: | | | | | |
| 4–16–4–200–3 | 36 | 41 | 50 | 53 | 55 |
| 4–16–4–650–3 | 39 | 44 | 51 | 54 | 58 |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| Стеклопакет: 6–98–6 | 40 | 42 | 45 | 48 | 50 |
| Окна телестудий: 10–8–10 | 63 | 71 | 66 | 73 | 77 |

*Примечание.* *) Стекло — воздушный зазор — стекло — воздушный зазор — стекло.

Из приведенных данных следует вывод о том, что звукоизоляция одинарного остекления соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении. Повышение звукоизоляции оконных проемов достигается:

- уплотнением притворов переплетов путем подгонки частей переплета между собой, уплотнением стекол с помощью прокладок из резины;
- применением уплотняющих прокладок между переплетом и коробкой, обеспечивающих плотное закрытие окон;
- облицовкой периметра межстекольного пространства звукопоглощающим материалом;
- установкой оконных блоков с повышенной звукоизоляцией (с двойным и тройным остеклением).

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения (см. табл. 23.3). Разработаны конструкции окон с повышенным звукопоглощением на основе стеклопакетов с герметизацией воздушного промежутка, с заполнением при пониженном давлении промежутка между стеклами различными газовыми смесями или созданием даже между ними вакуума. Уплотнение частей окон повышает их звукоизоляцию приблизительно на 10 дБ, при облицовке межстекольного пространства по периметру звукопоглощающим покрытием она увеличивается еще примерно на 5 дБ.

Побелка (окраска) потолков, навесные потолки, паркет (ламинат, линолеум), ковер (ковролин) на полу увеличивают звукоизоляцию перекрытий.

Для снижения опасного акустического сигнала в помещениях применяют также **акустические экраны**, размещаемые на пути распространения звука. Акустические экраны устанавливают на опасных направлениях распространения акустической волны с защищаемой информацией. Эффективность экрана повышается с увеличением соотношения его линейных размеров и длины акустической волны. Размеры экранов должны превышать более чем в 2–3 раза длину волны. Реально достигаемая эффективность акустических экранов, покрытых звукопоглощающими материалами, составляет 8–10 дБ.

Акустические экраны могут использоваться для дополнительной защиты дверей, окон, технологических проемов, панелей кондиционеров, отверстий воздушной вентиляции и других конструкций, имеющих не удовлетворяющую действующим нормам локальную звукоизоляцию. Применение акустических экранов целесообразно также для защиты акустической информации в помещениях временного использования, когда их капитальный ремонт нецелесообразен.

Для звукоизоляции по всем направлениям в ограниченном пространстве применяют **кабины** (для людей) и **кожуха** (для излучающих звуки механизмов и машин). Основное отличие звукоизолирующего кожуха от кабины заключается в необходимости обеспечения в кабине условий для пребывания в ней человека — вентиляции воздуха, освещения, средств связи.

В конструктивном отношении звукоизолирующие кабины делятся на **каркасные** и **бескаркасные**. В первом случае на металлическом каркасе крепятся звукопоглощающие панели. Примером таких кабин являются кабины междугородной телефонной связи. Кабина с двухслойными звукоглощающими плитами обеспечивает ослабление звука до 35–40 дБ. Более высокой акустической эффективностью обладают кабины бескаркасного типа. Они собираются из готовых многослойных щитов, соединенных между собой через звукоизолирующие упругие прокладки. Такие кабины дорогие в изготовлении, но снижение уровня звука в них может достигать 50–55 дБ. Для повышения звукоизоляции минимизируют возможное число стыковочных соединений отдельных панелей между собой и с каркасом кабины, стыки тщательно герметизируют и уплотняют, применяют звукопоглощающие облицовки стен и потол-

ка, глушат звуки средств вентиляции и кондиционирования воздуха.

Перспективными кабинами являются **прозрачные переговорные кабины**. Двухслойные ограждающие поверхности и стыковочные узлы этих кабин, а также мебель (столик и стулья) изготавливают из органического стекла. Прозрачность ограждений и мебели позволяет быстро обнаруживать закладные устройства и контролировать во время переговоров пространство вокруг кабины. Например, кабина Л-44 и различные модификации кабины Л-45 предназначены для 2–8 человек, имеют площадь внутри кабины 4–8 м$^2$, обеспечивают звукоизоляцию в диапазоне 300–5000 Гц не менее 25 дБ. В дальнейшем предполагается нанесение на поверхность кабины прозрачных композитивных пленок на лавсановой основе, что обеспечит одностороннюю (из кабины) проводимость света, почти в 20 раз увеличит механическую прочность прозрачных ограждающих конструкций, вдвое повысит устойчивость поверхности огню, исключит возможность лазерного подслушивания.

Звукоизолирующие кабины в зависимости от требований к изоляции звука подразделяются на 4 класса. Кабины 1-го класса должны обеспечивать ослабление звука в диапазоне 63–8000 Гц на 25–50 дБ, 2-го класса на 15–49 дБ в том же диапазоне, 3-го и 4-го классов — до 39 и 29 дБ соответственно. Наименьшие значения соответствуют низким частотам, наибольшее ослабление происходит на частотах 2000–4000 Гц.

**Звукоизолирующие кожуха** проще по конструкции и изготовляются из листовых материалов (стали, дюралюминия и др.). Поверхность стенок кожухов облицовываются звукопоглощающими материалами толщиной 30–50 мм в виде матов из минеральной ваты, супертонкого стекла или базальтового волокна.

Кожух для блокирования передачи структурного звука устанавливается на виброизолирующих прокладках. Внутри кожуха помещаются источники звука. Кожуха бывают съемными, раздвижными и капотного типа, сплошной герметичной или неоднородной конструкции — со смотровыми окнами, открывающими дверцами, проемами для ввода коммуникаций, циркуляции воздуха. Кожуха снижают уровень звука на 20–40 дБ.

В зависимости от способа глушения звука глушители подразделяются на **абсорбционные, реактивные** и **комбинированные**.

В абсорбционных глушителях происходит звукопоглощение в материалах и конструкции, в реактивных — в результате отражения звука обратно к источнику. Комбинированные глушители объединяют оба этих способа.

Звукопоглощение обеспечивается путем преобразования в звукопоглощающем материале кинетической энергии в тепловую. Звукопоглощающие материалы имеют волокнистое, зернистое или ячеистое строение с различной степенью жесткости. Поглощающая способность звукопоглощающих материалов обусловлена их пористой структурой, содержащей большое количество (не менее 75%) открытых сообщающихся между собой пор диаметром не более 2 мм. Стенками пор создается большая удельная поверхность звукопоглощающих материалов, при взаимодействии с которой звуковые колебания преобразуются в тепловую энергию вследствие потерь на трение между частицами материала.

Пористые материалы представляют звукопоглощающие облицовки в виде акустических плит мелкой зернистой или ячеечной структуры (плиты минераловатные «Акмигран», «Акмант», «Силакпор», «Винипор», ПА/С, ПА/О, ПП-80, ППМ, ПММ) и штучные звукопоглотители. Плоский слой звукопоглощающего материала облицовок устанавливается на жестком основании, которое крепится непосредственно или с воздушным промежутком на поверхности ограждения, к потолку или стенам. Штучные поглотители представляют собой одно- или многослойные объемные звукопоглощающие конструкции (в виде куба, параллелепипеда, конуса), подвешиваемые к потолку помещения. Размеры граней штучных звукопоглотителей составляют 40–400 см.

По степени жесткости звукопоглощающие материалы делятся **на мягкие, полужесткие и жесткие**.

Мягкие звукопоглощающие материалы изготавливаются на основе минеральной ваты или стекловолокна в виде матов и рулонов с объемной массой до 70 кг/м$^3$, которые обычно применяются в сочетании с перфорированным листовым экраном из алюминия, асбестоцемента, жесткого поливинилхлорида и др. или покрываются пористой пленкой. Они имеют коэффициент поглощения 0,7–0,85.

Полужесткие материалы представляют собой минераловатные или стекловолокнистые плиты с объемной массой 80–130 кг/м$^3$, древесно-волокнистые плиты с объемной массой 180–300 кг/м$^3$, а

также плиты из пористых пластмасс из пенополиуретана, полистирольного пенопласта и др. Поверхность плит покрывается пористой краской или пленкой. Коэффициент поглощения полужестких материалов составляет 0,65–0,75.

Твердые материалы изготавливаются на основе гранулированной или суспензированной минеральной ваты и коллоидного связывающего вещества (крахмального клейстера, раствора карбоксиметилцеллюлозы), в виде плит, в состав которых входят пористые заполнители (вспученный перлит, вермукулит, пемза) и белые или цветные портланд-цементы, а также плит из фибролита. Поверхность плит окрашена и имеет различную фактуру (трещиноватую, рифленую, бороздчатую). Объемная масса твердых звукопоглощающих материалов составляет 300–400 кг/м$^3$ и коэффициент поглощения — 0,6–0,7.

Для повышения звукопоглощающей способности ограждений (стен, потолка, дверей) применяют пористые материалы с жестким каркасом (в виде плиток на пемзолите, оштукатуренных плит с заполнителем, плит из цементного фибролита), с полужестким каркасом в виде древесно-волокнистых и минерально-ватных плит, с упругим каркасом из полиуретанового пенопласта, пористого поливинихлорида, прошитых и обернутых в ткань маты из капронового волокна. Они укрепляются с воздушным зазором на поверхности ограждений или между ограждениями с недостаточным звукопоглощением.

Коэффициенты звукопоглощения α типовых пористых поглотителей указаны в табл. 23.5.

*Таблица 23.5*

| *Поглотители* | *b, мм* | *α в зависимости от частоты, Гц* | | | | | |
|---|---|---|---|---|---|---|---|
| | | *250* | *500* | *1000* | *2000* | *4000* | *6000* |
| Минерально-ватные | 50 | 0,40 | 0,72 | 0,98 | 0,97 | 0,79 | 0,75 |
| Древесно-волокнистые | 50 | 0,30 | 0,34 | 0,32 | 0,41 | 0,42 | 0,42 |
| Маты из стекловолокна | 50 | 0,26 | 0,64 | 0,89 | 0,75 | 0,78 | 0,84 |
| Маты из минеральной ваты | — | 0,59 | 0,99 | 0,98 | 0,96 | 0,87 | 0,84 |
| Тарная ткань в сборку | 50 | 0,28 | 0,46 | 0,60 | 0,58 | 0,60 | 0,68 |

*Примечание.* b — зазор между отражателем и поглотителем.

Из анализа данных таблицы следует, что большинство пористых поглотителей имеют резонансные свойства в речевом диапазоне частот.

Существенное повышение звукопоглощения обеспечивают многослойные панели из комбинации плотных (из гипсо-волокнистых плит) и размещаемых между ними рыхлых легких слоев из минеральной и (или) стеклянной ваты различной толщины. В зависимости от требований количество слоев таких звукоизолирующих панелей составляет от 2 до 6, а толщина панелей — 40–130 мм.

Отдельную группу образуют **мембранные** и **резонаторные звукопоглотители**. Мембранные поглотители представляют собой тонкие плотные материалы — натянутую ткань, тонкую фанеру, картон и др., образующие мембраны, за которыми укрепляется хорошо демпфирующий материал (поролон, губчатая резина, войлок, минеральная вата и др.). Поглощение осуществляется на резонансных частотах поглотителя, величины которых зависят от геометрических размеров, плотности материала мембраны и силы ее натяжения. Значения коэффициентов звукопоглощения мембранных поглотителей приведены в табл. 23.6.

*Таблица 23.6*

| *Поглотитель* | *d*, *мм* | *b*, *мм* | *α в зависимости от частоты, Гц* | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | *250* | *500* | *1000* | *2000* | *4000* | *6000* |
| Фанера | 100 | — | 0,39 | 0,18 | 0,18 | 0,13 | 0,12 | 0,10 |
| Древесно-стружечный | — | — | 0,09 | 0,09 | 0,08 | 0,09 | 0,14 | 0,14 |
| Бумажно-слоистый | 150 | — | 0,38 | 0,22 | 0,14 | 0,02 | — | — |
| Дюралюминиевый | 50 | 50 | 0,34 | 0,16 | 0,08 | 0,02 | — | — |
| Сухая гипсовая штукатурка | — | 50 | 0,31 | 0,13 | 0,09 | 0.06 | 0.13 | 0.04 |
| Пенопласт | — | — | 0,02 | 0,19 | 0,16 | 0.14 | 0.12 | 0,12 |

*Примечание.* d — толщина заполнителя, b — зазор между поглотителем и отражателем.

К резонаторным поглотителям относятся перфорированные акустические экраны, образующие систему воздушных резонато-

ров. Простейшим резонаторным поглотителем является деревянный лист с равномерно распределенными на его поверхности отверстиями (перфорациями), расположенный на определенном расстоянии от стены. Резонансная частота для такого поглотителя определяется по формуле:

$$f = \frac{c}{2\pi}\sqrt{\frac{S}{\delta_э d^2 h}},$$

где S — сечение отверстия; c — скорость структурного звука в дереве; $\delta_э = \delta + 0{,}5\sqrt{\pi S}$ — эффективная толщина листа; δ — толщина листа; h — расстояние от стены или потолка; d — расстояние между отверстиями.

Перфорированные резонаторные поглотители применяют, прежде всего, для уменьшении энергии акустической волны, падающей на нагревательные конструкции (отопительные батареи, панели, стены). Они состоят из перфорированных листов металла, древесно-волокнистых и асбестоцементных плит, фанеры и других материалов, оклеенных с обратной стороной тканью. Характеристики поглотителей выбираются такими, чтобы, с одной стороны, обеспечить требуемое поглощение речевого акустического сигнала, а с другой стороны, не затруднять движение теплого воздуха.

Значения коэффициентов звукопоглощающих резонаторных поглотителей указаны в табл. 23.7.

*Таблица 23.7*

| *Поглотители* | *d, мм* | *b, мм* | *α в зависимости от частоты, Гц* | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | *250* | *500* | *1000* | *2000* | *4000* | *6000* |
| Фанера, 5 мм | 100 | 100 | 0,52 | 0,27 | 0,14 | 0,12 | 0,10 | 0,10 |
| Фанера 20 мм | 100 | 100 | 0,98 | 0,95 | 0,50 | 0,32 | 0,27 | 0,28 |
| Слоистый пластик, подклеенный марлей | — | 50 | 0,32 | 0,35 | 0,12 | 0,07 | — | — |
| Дюралюминий 5 мм | 50 | 50 | 0,89 | 0,99 | 0,47 | 0,15 | 0,04 | — |
| Акустические плиты гипсованные | 50 | — | 0,47 | 0,98 | 0,73 | 0,44 | 0,41 | 0,41 |
| Акустические плиты гипсованные, подклеенные бязью | 50 | — | 0,69 | 0,94 | 0,76 | 0,51 | 0,43 | 0,42 |

В реальных условиях применяются комбинации различных звукопоглощающих материалов. Коэффициенты поглощения некоторых широко применяемых материалов на частотах речевого диапазона приведены в табл. 23.8.

*Таблица 23.8*

| *Материал* | *Коэффициент поглощения α на частотах, Гц* | | | | |
|---|---|---|---|---|---|
| | *250* | *500* | *1000* | *2000* | *4000* |
| Кирпичная стена | 0,025 | 0,032 | 0,041 | 0,049 | 0,07 |
| Деревянная обивка | 0,11 | 0,11 | 0,08 | 0,082 | 0,11 |
| Стекло одинарное | — | 0,027 | — | 0,02 | — |
| Штукатурка известковая | 0,04 | 0,06 | 0,085 | 0,043 | 0,058 |
| Войлок (толщина 25 мм) | 0,36 | 0,71 | 0,8 | 0,82 | 0,85 |
| Ковер с ворсом | 0,08 | 0,21 | 0,27 | 0,27 | 0,37 |
| Стеклянная вата (толщиной 9 мм) | 0,4 | 0,51 | 0,6 | 0,65 | 0,6 |
| Хлопчатобумажная ткань | 0,04 | 0,11 | 0,17 | 0,24 | 0,35 |

Для акустической обработки помещений с целью уменьшения чрезмерно большого времени реверберации к потолку подвешивают штучные объемные звукопоглощающие средства в виде щитов, конусов, призм, шаров, параллелепипедов. Их выполняют из перфорированных листов твердого картона, пластмассы, металла, алюминиевой фольги, которые оклеиваются изнутри войлочной тканью или пористым звукопоглощающим материалом.

Обеспечение рациональных значений рассмотренных условий достигается как общим количеством звукопоглощающих материалов в помещении, так и распределением звукопоглощающих материалов по ограждающим конструкциям с учетом конфигурации и геометрических размеров помещения.

## 23.2. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств

### 23.2.1. Классификация средств обнаружения и локализации закладных подслушивающих устройств

Вследствие постоянной конкуренции между производителями закладных устройств и средств их обнаружения и локализации на рынке существует множество видов и типов технических средств, как тех, так и других. Классификация технических средств обнаружения и локализации закладных устройств приведена на рис. 23.2.

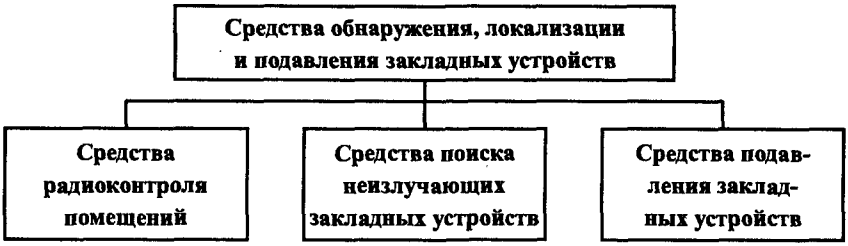



*Рис. 23.2.* Классификация средств обнаружения и локализации закладных устройств

Средства радиоконтроля помещения предназначены для обнаружения закладных устройств, излучающих радиоволны во время их поиска. Для обнаружения не излучающих при поиске закладок — дистанционно управляемых и передающих сигналы по проводам применяются средства, реагирующие не на радиоизлучения, а на иные демаскирующие признаки закладок. Наконец, средства подавления закладных устройств обеспечивают энергетическое скрытие их сигналов, нарушение работоспособности закладок или их физическое разрушение.

Учитывая, что радиоизлучающие закладки преобладают на рынке закладных устройств, существуют разнообразные средства радиоконтроля обследуемых помещений: от простейших индикаторов электромагнитного поля до сложных автоматизированных

комплексов. Классификация обнаружителей радиоизлучений закладных устройств указана на рис. 23.3.

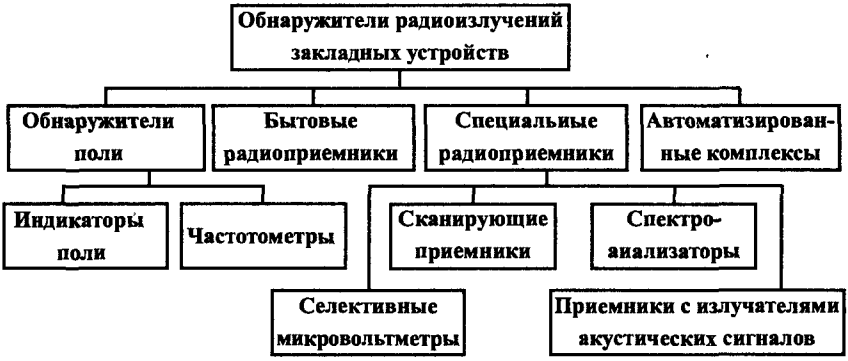



*Рис. 23.3.* Классификация средств обнаружения излучений закладных устройств

Простейшими и наиболее дешевыми обнаружителями радиоизлучений закладных устройств являются **обнаружители электромагнитных полей**. Наиболее простые из них — индикаторы поля, которые световым или звуковым сигналом информируют оператора о наличии в месте расположения антенны индикатора электромагнитного поля с напряженностью выше фоновой. Более сложные из них — частотомеры обеспечивают, кроме того, измерение частоты колебаний поля. Но чувствительность обнаружителей поля мала, поэтому с их помощью можно обнаруживать поля радиозакладок в непосредственной близости от источника излучения.

Существенно большую чувствительность имеют **супергетеродинные бытовые приемники**. Однако возможности использования бытовых радиоприемников для поиска радиозакладок ограничены радиовещательным диапазоном и видами модуляции, применяемыми в радиовещании (АМ и ЧМ). С помощью преобразователей (конверторов) можно перестроить частотный диапазон бытового радиоприемника на частоту радиозакладки, если она известна. Но для поиска радиозакладных устройств с неизвестной частотой перестроенные бытовые радиоприемники неэффективны, так как они обеспечивают поиск частоты закладки в узком диапазоне частот.

Широкими возможностями по обнаружению радиозакладок обладают **специальные приемники**. Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок — от долей МГц до единиц ГГц.

Время просмотра диапазона частот удается значительно сократить в радиоприемниках с электронной перестройкой частоты и блоками памяти в так называемых **сканирующих приемниках**. Блоки памяти этих приемников позволяют запоминать частоты сигналов, о которых достоверно известно, что они не принадлежат закладным устройствам.

Информационно-техническое сопряжение сканирующих приемников с переносными компьютерами послужило технической основой для создания **автоматизированных комплексов** для быстрого и надежного поиска радиоизлучающих подслушивающих устройств. Время просмотра диапазона частот удается значительно сократить в радиоприемниках с электронной перестройкой и блоками памяти. Блоки памяти этих приемников позволяют запоминать частоты сигналов, о которых достоверно известно, что они не принадлежат закладным устройствам. Для дальнейшего сокращения времени просмотра диапазона частот и повышения вероятности обнаружения сигналов закладных устройств применяют следующие дополнительные меры:

- повышают скорость сканирования до 100 МГц/с и более;
- осуществляют аналогово-цифровую обработку сигналов на базе процессора быстрого преобразования Фурье;
- производят автоматический панорамный анализ сигналов участка диапазона шириной до 15–20 МГц путем идентификации спектрограмм текущих сигналов с заложенными в память эталонными спектрограммами сигналов закладных устройств;
- используют в качестве признака идентификации сигнала закладного устройства тестовые акустические сигналы, излучаемые специальным акустическим генератором комплекса и ретранслируемые закладным устройством;
- автоматически определяют координаты закладного устройства по времени запаздывания на мембране его микрофона тестовых акустических сигналов от акустических колонок комплекса.

Но дистанционно управляемые радиозакладки и закладки, передающие информацию по проводам, не обнаруживаются аппара-

турой радиоконтроля. Для их поиска используются демаскирующие признаки материала конструкции и элементов схемы закладного устройства, а также признаки сигналов, распространяющихся по проводам. С целью обнаружения и локализации таких закладок применяются или создаются специальные технические средства, классификация которых приведена на рис. 23.4.

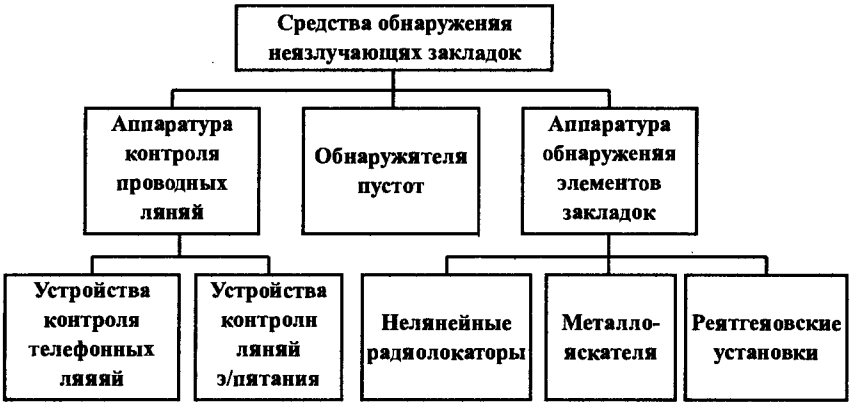



*Рис. 23.4.* Классификация средств обнаружения неизлучающих закладок

**Аппаратура для контроля проводных линий** предназначена для выявления в них опасных сигналов и их источников, в том числе закладных устройств. Так как основными направляющими линиями, по которым передаются от закладных устройств электрические сигналы с информацией, являются телефонные линии и цепи электропитания, то соответствующие средства контроля включают приборы контроля телефонных линий и линий электропитания.

**Обнаружители пустот** позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройствах, металлические детали конструкции, элементы, поглощающие рентгеновские лучи.

Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам — **нелинейные радиолокаторы**. Принципы работы нелинейных радиолокаторов близки к принципам работы радиолокационных станций, широко применяемых для радиолокационного наблюдения различных объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта эхосигнал на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники переизлученного (отраженного) сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик выход/вход полупроводников. В результате нелинейного преобразования электрического сигнала, индуцируемого в элементах схемы закладного устройства высокочастотным полем локатора, образуется сигнал, в спектре которого присутствуют кроме основной частоты ее гармоники. Количество и амплитуда гармоник зависят от характера нелинейности и мощности электромагнитного поля.

**Металлодетекторы (металлоискатели)** реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

**Переносные рентгеновские установки** применяются для просвечивания предметов, назначения которых не удается выявить без их разборки, прежде всего тогда, когда разборка невозможна без разрушения найденного предмета.

### 23.2.2. Аппаратура радиоконтроля

Принципы работы и основные характеристики средств радиоконтроля состоят в следующем.

**Обнаружитель поля** представляет собой широкополосный приемник прямого усиления (в простейшем случае — детекторный) с телескопической штыревой антенной. Усиленные сигналы, превышающие по уровню вручную устанавливаемое пороговое значение, подаются на световой и звуковой индикаторы, информирующие оператора о наличии в месте нахождения антенны электромагнитного поля с мощностью, превышающей пороговое

значение. Перед поиском закладки индикатор поля настраивается на уровень фона в обследуемом помещении. С этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок, устанавливает регулятор чувствительности в такое положение, при котором индикатор находится на грани срабатывания. При приближении индикатора поля к излучающей закладке напряженность электромагнитного поля возрастает, повышается уровень сигнала в антенне и, соответственно, на входе индикатора поля. При превышении уровня порогового значения, определяемого положением регулятора чувствительности, индикатор срабатывает, оповещая о появлении в обследуемой зоне электромагнитного поля мощностью, превышающей мощность фона. С целью большей информативности световых индикаторов их выполняют в современных обнаружителях поля в виде линейки из 4–10 светодиодов. Каждый последующий светодиод излучает свет при повышении уровня электромагнитного поля.

В силу широкой полосы детекторного приемника, существенно превышающей ширину спектра сигнала, чувствительность этих средств невелика и составляет единицы мВ. Кроме того, в помещении за счет многократных переотражений электромагнитных волн различных источников образуются «стоячие» волны, которые могут маскировать излучение закладного устройства небольшой мощности и пучности которых могут обнаруживать индикаторы поля. Для повышения возможностей индикаторы поля дополнятся счетчиками частоты сигнала максимальной амплитуды, индикаторами уровня, малогабаритными громкоговорителями для обеспечения «акустической завязки». Последняя достигается подачей усиленного демодулированного сигнала на громкоговоритель. При приближении индикатора поля с громкоговорителем, излучающим шумовой акустический шум, к скрытно установленному закладному устройству этот акустический сигнал им переизлучается и после детектирования и усиления озвучивается громкоговорителем. Возникает положительная акустическая обратная связь, которая приводит к резкому возрастанию громкости шумового акустического сигнала по мере приближения к закладному устройству. Такой индикатор поля позволяет не только примерно определить местонахождение источника излучения повышенной мощности,

но и с высокой достоверностью идентифицировать закладное устройство. Хотя вероятность обнаружения закладного устройства с помощью обнаружителя поля невелика, простота схемы, низкая стоимость, малые размеры и масса обнаружителей поля обеспечивают их широкое применение в качестве средств поиска закладных радиоизлучающих в ходе визуального осмотра помещения, особенно в труднодоступных местах (под плинтусом, за картиной, в книжном шкафу и др.).

В результате дальнейшего развития индикаторов поля созданы широкополосные радиоприемные устройства — **интерсепторы** с автоматической настройкой их селективных элементов на радиосигнал с наибольшим уровнем. Чувствительность интерсепторов выше чувствительности детекторных индикаторов поля. Например, интерсептор AS104 фирмы Optoelectronics обеспечивает прием радиосигналов в полосе 10–1000 МГц, имеет активный преселектор с полосой 4 МГц и усиление в 30 дБ.

Принцип «захвата» частоты радиосигнала с максимальным уровнем и последующим анализом его характеристик микропроцессором положен в основу работы современных **частотомеров**. Микропроцессор записывает сигнал с максимальным уровнем во внутреннюю память, производит его цифровую фильтрацию, проверку на стабильность и когерентность сигнала и измерение его частоты с точностью до единиц кГц (2 кГц, 0,01% от номинального значения). Значение частоты в цифровой форме индуцируется на жидкокристаллическом экране.

Знание частоты позволяет оператору грубо классифицировать принимаемый радиосигнал по возможным его источникам (радио- или телевизионное вещание, служебная связь, сотовая радиотелефонная связь и т. д.) и повысить оперативность «чистки» помещения.

**Бытовые приемники** как средства обнаружения закладных устройств имеют существенно более высокую чувствительность, чем индикаторы поля и частотомеры, и позволяют уверенно принимать радиосигнал закладки, если только его частота соответствует диапазону частот радиоприемника. Диапазоны частот бытовых радиоприемников стандартизированы и составляют: для России и стран СНГ 65,8–74 Мгц (УКВ1) и 100–108 Мгц (УКВ2), в соответствии

с Международным регламентом радиосвязи 41–68 Мгц (УКВ1) и 87,5–108 Мгц (УКВ2). Большинство современных бытовых радиоприемников выпускаются в так называемом расширенном диапазоне 65–108 Мгц. Доля закладок с частотами излучений, попадающих в эти диапазоны, мала и постоянно убывает. Учитывая это, некоторые бытовые радиоприемники оснащаются встроенными или подключаемыми конверторами (преобразователями) на диапазон излучений радиозакладок до 450–480 МГц. К таким приемникам относятся, например, AE 1490, Sony CFM-145. У них имеется дополнительный диапазон рабочих частот 460–480 МГц, чувствительность их составляет 2–3 мкВ, что обеспечивает прием высокочастотных ЧМ-сигналов радиозакладок.

Наглядное представление о загрузке радиодиапазона, что облегчает поиск радиозакладных устройств, обеспечивают **анализаторы спектра**. Широкий диапазон частот имеют анализаторы спектра производства фирмы Rohde&Schwarz ZWOB2 (100 кГц–1,6 кГц), ZWOB6 (100 кГц–2,7 ГГц), ZWOB4 (100 кГц–2,3 ГГц), ZRMD (10 МГц–18 ГГц). Несколько меньшими возможностями обладают анализаторы спектра производства стран СНГ: СК4-61 (100 МГц–15 ГГц), С4-42 (40 МГц–17 ГГц), СК4-59 (10 кГц–0,3 ГГц), С4-47 (100 МГц–39,6 ГГц), СК4-83 (10 Гц–0,3 Гц), С4-9 (50 МГц–1,4 МГц).

Все более широко для поиска закладных устройств применяются **сканирующие радиоприемники**. Эти приемники имеют высокие электрические параметры в широком диапазоне частот настройки, перекрывающем частоты радиоизлучений имеющихся на рынке закладок. Сканирующие приемники автоматически последовательно настраиваются на частоты радиосигналов во всем диапазоне. Оператор, прослушивая звуковые сигналы на выходе приемника на каждой из частот, принимает решение о продолжении или прекращении поиска. Для продолжения поиска он нажимает соответствующую кнопку, подавая устройству управления приемника команду о перестройке на следующую частоту. В сканирующих приемниках с памятью в ней запоминаются частоты радиосигналов, которые не интересуют оператора, что ускоряет процесс последующего поиска. Очевидно, что для того, чтобы оператор мог обнаружить радиосигнал закладки, она должна передавать узнаваемый

акустический сигнал. Для этого при поиске закладок с помощью бытовых и сканирующих радиоприемников необходимо в обследуемом помещении излучать акустический сигнал. Акустический сигнал, кроме того, «провоцирует» закладные устройства, автоматически включаемые от голосов разговаривающих.

В условиях большого и постоянно расширяющегося диапазона частот излучений радиозакладных устройств его последовательный просмотр даже с помощью сканирующих приемников занимает несколько часов. В результате длительного поиска оператор утомляется и повышается вероятность пропуска им излучения закладки. Для оперативного поиска закладок применяются **специальные приемники**, которые содержат кроме сканирующего приемника излучатель акустического тестового сигнала и микропроцессор. Излучатель акустического сигнала имитирует источник акустической информации. Микропроцессор выявляет радиосигналы, на которые настраивается сканирующий приемник, по критерию «свой–чужой» и быстро обнаруживает радиосигнал закладки, если таковой имеется. Например, приемник PK 855-S генерирует звуковой сигнал на частоте 2,1 кГц. После обнаружения «своего» сигнала он последовательно автоматически проверяет его 4 раза, после чего подается сигнал оператору об обнаружении закладки. Сканирование всего диапазона частот занимает около 3–4 минут. Чтобы избежать перегрузки чувствительных микрофонов и надежно обнаруживать радиозакладки различных типов, громкость тестового акустического сигнала ступенчато меняется: 1,5–2 мин он излучается на полной громкости, затем то же время на половинной мощности. Аппаратура размещается в портфеле типа «дипломат», весит 4,9 кг.

Дальнейшее развитие специальных приемников привело к появлению на рынке **автоматизированных программно-аппаратных комплексов** для поиска средств негласного съема акустической информации. Типовой комплекс включает:

- сканирующий радиоприемник с широкополосными антеннами;
- коммутатор антенн для комплексов, контролирующих несколько помещений;
- компьютер типа Notebook или микропроцессор;
- специальное математическое и программное обеспечение комплекса;

- контролер ввода информации с выхода радиоприемника в компьютер и формирования тестового сигнала;
- преобразователь спектра;
- акустический коррелятор;
- блок питания.

Комплекс при минимальном участии оператора определяет и запоминает уровни и частоты радиосигналов в контролируемом помещении, выявляет в результате корреляционной обработки спектрограмм вновь появившиеся излучения, с использованием тестового акустического сигнала распознает скрытно установленные в помещении радиомикрофоны и определяет их координаты. Возможности комплексов расширяют также включением в их состав блока контроля проводных линий, позволяющего обнаруживать подслушивающие устройства, подключенные к проводам кабелей.

В комплект современных автоматизированных комплексов радиомониторинга включают генератор прицельных помех. Он обеспечивает возможность оперативно настраиваться на частоту обнаруженного закладного устройства и подавлять его сигналы в условиях, когда нет времени на поиск и нейтрализацию закладного устройства, например, во время совещания.

С целью сокращения времени просмотра диапазона частот до нескольких минут анализ сигналов в перспективных комплексах проводится на основе быстрого преобразования Фурье.

Создание и применение автоматизированных комплексов для непрерывного радиомониторинга помещений с конфиденциальной информацией является наиболее эффективным направлением развития средств для комплексной защиты информации от утечки по радиоэлектронному каналу.

Такое утверждение основывается на следующих предпосылках:

- при непрерывном контроле накапливается большой объем информации об электромагнитной обстановке в защищаемом помещении, что облегчает и ускоряет процесс обнаружения новых источников излучения;
- выявляются не только непрерывно излучающие или включаемые по акустическому сигналу закладки, но и радиоизлучения дистанционно управляемых закладок в период их активной ра-

боты, т. е. создаются предпосылки для борьбы с закладными устройствами в реальном масштабе времени;

- выявляются информативные побочные излучения различных радиоэлектронных средств, для обнаружения которых в виду большей неопределенности их проявления и малой мощности излучений требуется более тщательный анализ радиообстановки в помещении.

Возможности автоматизированных комплексов определяются не столько техническими параметрами аппаратуры (большинство комплексов имеют близкие параметры, так как комплектуются в основном однотипными радиоприемниками и ПЭВМ), сколько программным обеспечением. Программные комплексы современных комплексов обладают большими возможностями: позволяют накапливать данные о радиоэлектронной обстановке, анализировать загрузку и спектральный состав радиосигналов в диапазоне частот радиоприемника, выявлять информативные электромагнитные излучения от любых РЭС, оценивать эффективность использования радиотехнических средств защиты информации и решать другие задачи.

Дальнейшее развитие автоматизированных комплексов предусматривает:

- расширение видов обнаруживаемых закладных устройств;
- создание и включение в состав программного обеспечения комплекса базы данных о закладных устройствах с информационными портретами излучаемых сигналов для их автоматического обнаружения и распознавания;
- разработку на базе программно-аппаратных средств комплексов экспертной системы по обнаружению источников утечки информации в радиоэлектронном канале.

### 23.2.3. Средства контроля телефонных линий и цепей электропитания

Учитывая повсеместное распространение телефонов как средств коммуникаций и повышенный интерес злоумышленников к подслушиванию телефонных разговоров, большое внимание при обеспечении защиты информации уделяется способам и средствам контроля телефонных линий.

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий и сигналов в них: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного ее сопротивлений. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного — в разрыв провода телефонного кабеля или параллельного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия. Наилучшие возможности по выявлению этих отклонений существуют при опущенной трубке телефонного аппарата. Это обусловлено тем, что в этом состоянии в телефонную линию подается постоянное напряжение 60 + 10% В (для отечественных телефонных линий) и 25–36 В (для зарубежных АТС). При поднятии трубки в линию поступают от АТС дискретный сигнал, преобразуемый в телефонной трубке в длинный гудок, а напряжение в линии уменьшается до 12 В.

Для контроля телефонных линий применяются следующие устройства:

- устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;
- измерители параметров телефонных линий (напряжения, тока, емкостного сопротивления, волнового сопротивления и др.), при отклонении которых от номинального значения формируется сигнал тревоги;
- «кабельные радары», позволяющие выявлять неоднородности телефонной линии и измерять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.).

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией изменения его значения от номинального, которое фиксируется оператором в режиме настройки вращением регулятора на лицевой панели уст-

ройства. Предполагается, что при установке номинального напряжения к телефонной линии подслушивающее устройство не подключено. Например, анализатор проводных линий АПЛ-1 («Иней», ассоциация «Конфидент») позволяет обнаруживать подключение подслушивающих устройств, включенных последовательно и имеющих сопротивление не менее 5 Ом, и подключенных параллельно с сопротивлением не более 1,5 мОм. На некоторых подобных устройствах, например ST1, устанавливается стрелочный измеритель напряжения (вольтметр), в других (АТ-23, «Атолл», АТЛ-2 и др.) предусмотрено цифровое отображение значений напряжения и тока на ЖК-дисплее.

Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет «микрофонного эффекта» в элементах телефонного аппарата и высокочастотного навязывания.

Но устройства контроля телефонной сети по изменению напряжения или тока в ней не обеспечивают надежного обнаружения подключаемых параллельно к линии современных средств подслушивания с входным сопротивлением более единиц МОм. Повышение реальной чувствительности устройств контроля ограничено нестабильностью параметров линии, колебаниями напряжения источников электропитания на АТС и помехами в линии. Для снижения вероятности ложных тревог в более сложных подобных устройствах увеличивают количество измеряемых характеристик линии, предусматривают возможность накопления и статистической обработки результатов измерений в течение достаточно длительного времени как контролируемой линии, так и близко расположенных. Например, портативный анализатор ССТО-1000 фирмы CCS Commucation Control позволяет проводить 6 типов контрольных проверок телефонной линии и может быть использован для одновременной проверки 25 телефонных пар, а анализатор АТЛ-2 информирует о размыкании телефонной линии на время более 20 секунд, которое возникает при последовательном подключении к ней подслушивающего устройства.

Так как любое физическое подключение к кабелю телефонной линии создает в ней неоднородность, от которой отражается посылаемый в линию сигнал, то по характеру отражения и времени

запаздывания отраженного сигнала оценивают вид неоднородности и рассчитывают длину участка линии до неоднородности (места подключения). В приборах АПЛ-1 и АТ-2 («Амулет», Москва) характер схемы подслушивающего устройства оценивается по фигуре Лиссажу, вид которой определяется сдвигом фаз между напряжением и током сигнала, подаваемого на вертикальные и горизонтальные пластины электронно-лучевой трубки. Для выявления неоднородностей применяют также испытатели кабельных линий Р5-А, Р5-5, Р5-8, Р5-9, Р5-10, Р5-13 и др.

Средствами и программным обеспечением для обнаружения и анализа сигналов закладных устройств в проводных линиях оснащаются также перспективные автоматизированные комплексы. Например, в мобильном автоматизированном комплексе «Крона 5» («Нелк») установлен многофункциональный конвертор, позволяющий обнаруживать утечку акустической информации по электросети, телефонным и другим проводным линиям в диапазоне частот 0,01–5 Мгц, а также по инфракрасному каналу.

Наиболее рациональным вариантом является совмещение в одном приборе функции обнаружения несанкционированного подключения к телефонной линии и противодействия подслушиванию. Активное противодействие осуществляется путем линейного зашумления телефонной линии.

### 23.2.4. Технические средства подавления сигналов закладных устройств

Другую группу средств активной борьбы с закладками образуют генераторы помех. Классификация этих средств приведена на рис. 23.5.

Выходы генератора линейного зашумления соединяются с проводами телефонной линии и электросети и в них подаются электрические сигналы, перекрывающие опасные сигналы по спектру и мощности. Генераторы пространственного зашумления повышают уровень электромагнитных помех в помещении и, следовательно, на входе приемника злоумышленника. Для эффективного подавления сигнала закладки уровень помехи в полосе спектра сигнала должен в несколько раз превышать уровень сигнала.

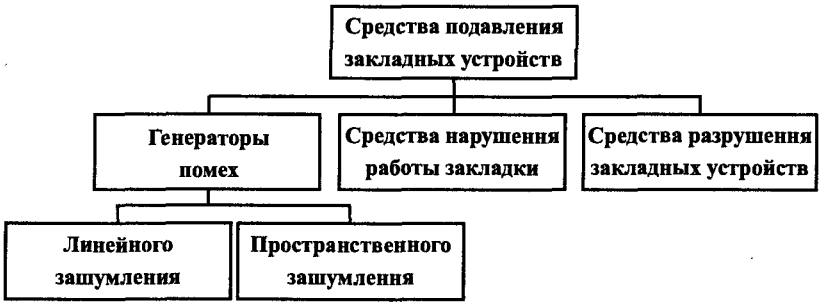



*Рис. 23.5.* Классификация средств подавления закладных устройств

Энергетическое скрытие информации путем подавления (снижения отношения сигнал/шум ниже порогового значения) электрических и радиосигналов позволяет обеспечить превентивную защиту информации без предварительного обнаружения и локализации закладных устройств. Возможны три способа подавления:

- снижение отношения сигнал/шум до безопасных для информации значений путем пространственного и линейного зашумления;
- воздействия на закладные устройства радио- и электрическими сигналами, нарушающими заданные режимы работы этих устройств;
- воздействия на закладные устройства, вызывающие их разрушение.

Для подавления сигналов закладных устройств применяются **заградительные** и **прицельные помехи**. Заградительные помехи имеют ширину спектра, перекрывающего частоты излучений подавляющего числа закладных устройств, — от долей до тысячи МГц. Мощность излучения не превышает 20 Вт («Гном-3»).

Однако подобные генераторы помех эффективно подавляют радиосигналы закладки, если отношение мощности помехи и сигнала закладки в несколько раз выше отношения ширины спектра помехи и сигнала. Это требование обусловлено тем, что мощность помехи «размазывается» по диапазону частот генератора помех, в среднем составляющем около 1000 МГц, и на долю узкополосного сигнала закладки приходится лишь незначительная часть энергии помехи, которой не хватает для эффективного искажения ин-

формационных параметров сигнала. Например, одно из устройств активной защиты информации с повышенной выходной мощностью обеспечивает максимальную мощность шума в полосе ЧМ-сигнала (150–200 кГц) порядка 40 мВт при интегральном значении выходной мощности генератора до 20 Вт. Но для узкополосного ЧМ-сигнала мощность помехи в полосе сигнала составляет доли и единицы мВт, что недостаточно для подавления сигналов закладки. Учитывая значительную долю на рынке радиозакладок с мощностью излучения порядка 10–20 мВт и тенденцию сужения полосы их кварцованных частот, применение даже достаточно мощных генераторов помех не гарантирует предотвращение утечки информации. Наращивание мощности заградительной помехи ограничивается требованиями по экологической безопасности и электромагнитной совместимости излучений помех и сигналов радиовещания и связи в зашумляемом пространстве.

Проблема электромагнитной совместимости не возникает при линейном зашумлении. Задача подавления сигналов закладок, передаваемых по цепям электропитания, решается простым превышением спектральной плотности помехи над спектральной плотностью сигнала. Для подавления телефонных радиозакладок путем линейного зашумления спектр помехи не должен совпадать со спектром речевого сигнала, иначе помеха будет мешать разговору абонентов. В качестве таких помех применяют аналоговые и дискретные помеховые сигналы, спектр которых выше спектра речевого сигнала. Простейшим дискретным помеховым сигналом является меандр — последовательность прямоугольных импульсов со скважностью 2. Частоты сигналов подбираются такими, чтобы они проходили через селективные цепи микрофонного усилителя и модулятора закладного устройства, но не воспринимались слуховой системой человека.

Сигналы-помехи с частотой выше 20 кГц изменяют режимы работы подключенных к телефонной линии закладных устройств, в результате чего изменяется частота и расширяется спектр их излучений. Вследствие этого ухудшается разборчивость принимаемой злоумышленником речи и уменьшается в несколько раз дальность подслушивания.

Воздействие помехи на параллельно подключенное к телефонной линии закладное устройство проявляется в основном в изме-

нении частоты излучения передатчика, в результате чего приемник, настроенный на номинальную частоту передатчика закладки, не сможет принять сигнал. Например, устройство защиты телефонных линий УЗТ-02 фирмы «Нелк» генерирует помеховый сигнал с максимальной амплитудой 35 В, который, воздействуя на элементы электронной схемы телефонной закладки, приводит к «размыванию» спектра излучаемого сигнала и снижению соотношения сигнал/шум на входе приемника злоумышленника. Воздействие помех нарушает также работу устройств автоматической регулировки уровня записи и автоматического включения диктофона голосом.

Один из способов физического повреждения закладок, подключенных к телефонной линии и линиям электропитания, — подача в линию коротких импульсов большой амплитуды. Так как в схемах закладок применяются миниатюрные низковольтные детали (транзисторы, конденсаторы), то высоковольтные импульсы их пробивают и схема закладки выводится из строя. Например, так называемый разрушитель «жучков» PK 3320 (PK Electronic) посылает в линию импульсы амплитудой до 4000 В и в течение 2–4 мин приводит в неработоспособное состояние закладное устройство. Отечественный выжигатель телефонных закладных устройств ПТЛ-1500 выводит из строя закладные устройства путем подачи в телефонную линию импульсов напряжением 1600 В. Однако метод физического разрушения аппаратных закладок нельзя использовать без отключения от телефонной линии всех радиоэлектронных средств (современных электронных телефонных аппаратов, модемов ПЭВМ, факсов и т. д.).

### 23.2.5. Нелинейные локаторы

На рынке имеется большой выбор моделей отечественных и зарубежных нелинейных локаторов. В зависимости от режима излучения их делят на локаторы с непрерывным и импульсным излучением. Проникающая глубина электромагнитной волны зависит от мощности и частоты излучения. Так как с повышением частоты колебаний увеличиваются затухания электромагнитной волны в среде распространения, то уровень мощности переотраженного сигнала тем выше, чем ниже частота локатора. Но при более низкой

частоте ухудшаются возможности локатора по локализации места нахождения нелинейности, так как при приемлемых размерах его антенны расширяется ее диаграмма направленности.

Очевидно, что чем выше мощность излучения локатора, тем глубже проникает электромагнитная волна и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения оказывает вредное воздействие на оператора. Для обеспечения его безопасности максимальная мощность излучения локатора в непрерывном режиме не должна превышать 3–5 Вт. При импульсном режиме работы локатора мощность в импульсе достигает 300 Вт при средней мощности, не превышающей долей и единиц Вт. Приемники нелинейных локаторов обеспечивают дальность обнаружения полупроводниковых элементов 0,5–2 и более метров и точность определения их местонахождения — несколько см (например, в локаторе «Родник» — 2 см). Максимальная глубина обнаружения объектов в маскирующей среде составляет десятки см, например локатор «Циклон» обнаруживает радиоэлектронные средства в железобетонных стенах толщиной 50 см, в кирпичных и деревянных стенах — до 70 см.

Отечественные локаторы по своим характеристикам не уступают, а некоторые образцы превышают показатели зарубежных, а по стоимости в несколько раз дешевле. Локатор «Обь» является полным аналогом зарубежных образцов. Радиолокаторы «Родник-ПМ», «Переход», «Энвис» имеют дополнительный режим анализа принятого от объекта сигнала, в том числе возможность прослушивания модулированных сигналов локатора, отраженных от полупроводниковых элементов закладок. Принцип модуляции аналогичен модуляции при высокочастотном навязывании. Локатор «Циклон» предоставляет возможность работы в двух режимах: в режиме поиска и в режиме «сторожа». В последнем режиме две антенны устанавливаются в проходе контрольно-пропускного пункта организации или в дверном проеме помещения, например зала заседания. Этот локатор позволяют дистанционно контролировать скрытый внос или вынос радиоэлектронных средств.

Нелинейные радиолокаторы обеспечивают высокую вероятность обнаружения закладных устройств всех типов, но являются достаточно сложными и дорогими средствами проверки помещения на отсутствие в них закладных устройств.

### 23.2.6. Обнаружители пустот, металлодетекторы и рентгеновские аппараты

Эта группа приборов использует физические свойства среды, в которой может размещаться закладное устройство, или свойства элементов закладных устройств, независимые от режима их работы.

Так как в пустотах сплошных сред (кирпичных и бетонных стенах, деревянных конструкциях и др.) могут устанавливаться долговременные дистанционно-управляемые закладные устройства, то выявление и обследование пустот проводится при «чистке» помещений.

В простейшем случае пустоты в стене или любой другой сплошной среде обнаруживаются путем их простукивания. Пустоты в сплошных средах изменяют характер распространения структурного звука, в результате чего воспринимаемые слуховой системой человека спектры звуков в сплошной среде и в пустоте отличаются.

Технические средства **обнаружения пустот** позволяют повысить достоверность выявления пустот. В качестве таких средств могут применяться как различные ультразвуковые приборы, в том числе медицинского назначения, так и специальные обнаружители пустот. Специальные технические средства для обнаружения пустот используют:

- отличия в значениях диэлектрической проницаемости среды и пустоты;
- различия в значениях теплопроводности воздуха и сплошной среды:
- отражения акустических волн в ультразвуковом диапазоне от границ раздела «твердая среда — воздух»).

В пустоте (воздухе) диэлектрическая постоянная близка к единице, для бетона, кирпича, дерева она значительно больше. Диэлектрики с разными значениями диэлектрической постоянной по-разному деформируют электрическое поле, создаваемое обнаружителем пустоты. По изменению диэлектрической индукции локализуется пустота. Так обнаружитель пустот «Кайма» выявляет полости в кирпичных или бетонных стенах размером 6 × 6 × 12 см и 6 × 6 × 25 см.

С помощью ультразвукового томографа Д 1230 обнаруживаются пустоты объемом от 30 см$^3$ на глубине до 1 м, ультразвукового толщинометра Д 1220 — глубиной до 50 см.

Эффективным средством выявления пустот в стенах, нагретых на несколько градусов выше температуры воздуха в помещении, являются тепловизоры. Чувствительность охлаждаемых тепловизоров достигает 0,01 градуса по Цельсию, неохлаждаемых — на порядок хуже. За счет разницы теплопроводности бетона или кирпича стен и воздуха границы пустот с воздухом при нагревании или охлаждении помещения могут наблюдаться на экране тепловизора.

Переносной неохлаждаемый тепловизор ТН-3 («Спектр») со встроенным цифровым процессором обеспечивает возможность наблюдения на экране изображений в ИК-диапазоне (8–13 мкм) объекта при минимальной разности температуры элементов его поверхности 0,15 град. Комплект тепловизора содержит камеру размером 110 × 165 × 455 мм и массой 6 кг, малогабаритный монитор и блок питания.

**Металлодетекторы** обнаруживают закладные устройства по магнитным и электрическим свойствам их элементов. Любая закладка содержит токопроводящие элементы: резисторы, индуктивности, соединительные токопроводники в навесном или микроминиатюрном исполнении, антенну, корпус элементов питания, металлический корпус закладки.

По принципу действия различают **параметрические (пассивные)** и **индукционные (активные) металлодетекторы**. По конструкции — **стационарные** и **ручные**. Для обнаружения малых токопроводящих элементов применяют в основном ручные металлодетекторы, которые можно приблизить вплотную к токопроводящему элементу.

В **параметрических металлодетекторах** токопроводящие элементы, попадающие в зону действия поисковой рамки (катушки) диаметром 250–300 мм, изменяют ее индуктивность. Эта катушка является индуктивностью колебательного контура поискового генератора, частота колебаний которого составляет 50–500 кГц. Чем выше частота колебаний генератора, тем больше отклонение частоты генератора, т. е. тем выше чувствительность металлодетекто-

ра, Но одновременно сильнее сказывается влияние среды, особенно грунта земли. Поэтому в некоторых типах металлодетектора поисковую катушку запитывают негармоническим сигналом с частотой 15–50 кГц, а для измерения отклонения частоты используются гармоники колебания на частотах 500–1000 кГц.

Для измерения отклонения частоты колебаний генератора параметрического металлодетектора широко применяется метод «биений» — явления, возникающего при сложении двух колебаний с близкими частотами. Одно колебание с изменяющейся частотой создается поисковым генератором, другое — эталонным генератором со стабилизированной частотой. Частоты этих колебаний устанавливаются равными при отсутствии в зоне действия поисковой рамки посторонних предметов. Частота биений поступает в виде тональной частоты на наушники и световой индикатор. По частоте тона звукового сигнала и миганий светового индикатора можно локализовать область, внутри которой находится металлический предмет.

Достоинством параметрических металлодетекторов является их магнитная селективность — способность разделять металлы по магнитным свойствам. Известно, что черные металлы (чугун, сталь, кобальт, сплавы) имеют удельную магнитную проницаемость $\mu >> 1$. У цветных парамагнитных металлов (титана, алюминия, олова, платины и др.) этот показатель незначительно больше 1, у диамагнитных металлов (золота, меди, серебра, свинца, цинка и др.) — незначительно меньше 1. Следовательно, по знаку и величине отклонения частоты поискового генератора от номинального (нулевого) значения можно судить о типе попавшего в зону действия рамки металлического предмета. Эта возможность расширила область применения ручных металлодетекторов, в том числе для поиска кладов, и активизировало исследования по их совершенствованию в середине 90-х годов XX в.

Однако чувствительность пассивных параметрических металлодетекторов недостаточна для обнаружения находящихся в неоднородной среде металлических предметов. Глубину обнаружения увеличивают в **индукционных металлодетекторах**. В них с помощью специального генератора и излучающей поисковой рамки (катушки) создают магнитное поле. Оно индуцирует в токопро-

водящих предметах вихревые токи, создающие вторичное поле. Это поле принимается другой, измерительной, катушкой металлодетектора. Наводимый в нем сигнал фильтруется, обрабатывается, усиливается и подается на звуковой и световой индикатор металлдетектора.

Различают аналоговые и импульсные индукционные металлодетекторы. В аналоговых металлодетекторах на поисковую катушку поступает от генератора гармонический сигнал с частотой 3–20 кГц. В импульсных металлодетекторах удается за счет мощного короткого импульса, подаваемого в поисковую катушку, сформировать магнитное поле с напряженностью 100–1000 А/м, на порядок превышающей напряженность поля аналогового металлодетектора и проникающей до 2 м в грунт земли.

Так как магнитное поле поисковой катушки пронизывает измерительную катушку, то основной технической проблемой индукционных металлодетекторов является компенсация сигналов, наводимых этим полем в измерительной катушке. Компенсация сигналов в измерительной катушке достигается за счет взаимно перпендикулярного пространственного расположения осей поисковой и измерительной катушек, использования компенсационной катушки с параметрами, идентичными параметрам измерительной, но с противоположным направлением намотки провода, а также путем соответствующей обработки сигналов.

Характеристики сигнала в измерительной катушке зависят от размеров токопроводящей поверхности объекта, ее электропроводности, магнитной проницаемости материала и частоты поля. Выделение очень слабых сигналов, наводимых в измерительной катушке металлодетектора вторичным полем мелких металлических предметов, на фоне различных помех, а также компенсация помех требует достаточно сложных алгоритмов оптимальной обработки, реализуемых микропроцессорной техникой.

Для обнаружения закладок применяются в основном ручные металлодетекторы. Измерительная и поисковая катушки в них могут выполняться в виде торроида диаметром порядка 140–150 мм, укрепленного на корпусе ручки (АКА 7202) или непосредственно в корпусе металлодетектора («Минискан»). Металлодетектор имеет звуковой и световой индикаторы, регулятор настройки чувстви-

тельности; питание ручных металлодетекторов от химических источников тока. Проблема автоматической подстройки коэффициента усиления металлодетектора под параметры среды решается микропроцессором. Максимальная чувствительность металлодетектора характеризуется обломком иглы длиной 5 мм, находящимся в поле действия измерительной катушки. Вес ручных металлодетекторов невелик: от 260 г до нескольких кг.

Для интерскопии предметов непонятного назначения применяют переносные **рентгеновские установки**. Переносные рентгеновские установки бывают двух видов:

- флюороскопы с отображением изображений на экране просмотровой приставки;
- рентгенотелевизионные установки.

**Переносные флюороскопы** состоят из излучателя, пульта дистанционного управления, просмотровой приставки с люминесцентным экраном, аккумуляторного блока, зарядного устройства, соединительных кабелей и сумок для переноса установки (транспортной упаковки). Обследуемый предмет размещается между излучателем и просмотровой приставкой на расстоянии около 50 см от излучателя и вплотную к просмотровой приставке.

Проникающая способность рентгеновских лучей пропорциональна анодному напряжению на рентгеновской трубке, которое достигает у некоторых переносных флюороскопов 250 кВ. Например, досмотровая рентгеновская установка «Шмель-90/К» фирмы «Флэш Электроникс» для обеспечения высокой проникающей способности имеет анодное напряжение 90 кВ. Она просвечивает стальную пластину толщиной 2 мм, бетонную стену толщиной до 100 мм, позволяет различить за преградой из алюминия толщиной 3 мм две медные проволоки диаметром 0,2 мм, расположенные на расстоянии 1 мм друг от друга. Рабочее поле экрана просмотровой приставки — круг диаметром 255 мм.

С целью повышения безопасности оператора в современных переносных рентгеновских флюороскопах (например, в флюороскопе Яуза-1 фирмы «Novo») используется люминесцентный экран с запоминанием, позволяющий рассматривать изображение после выключения высокого напряжения. В состав таких комплексов включается специализированный термоконтейнер для стирания изображения с люминесцентных экранов.

Уменьшение мощности рентгеновского излучения и масса-габаритных характеристик установки достигается усилением яркости изображения экрана. Переносной рентгеновский флюороскоп ФП-1 («Спектр») с коэффициентом усиления яркости экрана не менее 30000 имеет малые размеры (270 × 240 × 920 мм) и массу (3 кг). В то же время размеры его флюороскопического экрана составляют 250 × 250 мм. Дополнительно к нему поставляется фото- или видеоприставка для документирования изображений.

Для просвечивания тонких предметов с неметаллическими корпусами применяют установки с радиоактивными изотопами низкой активности. Такие установки компактны, просты в управлении и безопасны. Например, рентгеновская микроустановка РК-990 с габаритами 220 × 210 мм и массой 1,7 кг просвечивает объект с размерами до 63 × 87 мм.

В **рентгенотелевизионных** установках теневое изображение преобразуется в телевизионное изображение на экране удаленного от излучателя монитора. Например, рентгеновский аппарат «Шмель-экспресс» обеспечивает возможность наблюдения изображения объекта как на экране монитора, удаленного до 2 м от рентгеновской установки, так и на экране просмотровой приставки комплекса «Шмель-90К». Размер экрана рентгенотелевизионного преобразователя 360 × 480 мм. Эта установка позволяет запоминать до 1000 изображений и обеспечивает информационно-техническое сопряжение с ПЭВМ.

Применение рентгеновских установок для исследования закладных устройств ограничивается сравнительно их высокой стоимостью.

### 23.2.7. Средства контроля помещений на отсутствие закладных устройств

Для обеспечения безопасности информации в помещении необходим постоянный контроль отсутствия в нем закладных устройств — «чистка» помещений. Целесообразны следующие виды «чистки»:

- оперативный визуальный осмотр помещения;
- профилактический периодический контроль с использованием технических средств поиска и локализации закладных устройств;

- разовый контроль помещения перед проведением в нем совещаний с высоким грифом секретности;
- проверка помещения после проведения капитального ремонта в нем;
- проверка различных новых предметов, размещаемых в помещении представительских подарков, предметов интерьера, радиоэлектронных средств и др.;
- радиомониторинг помещения в течение рабочего времени, особенно во время совещания.

Частота и способы проверки помещений с целью выявления в них закладных устройств зависят от их категории и порядка допуска в них посторонних лиц. Наибольшее внимание службы безопасности требуют кабинеты руководителя и его ближайших заместителей. В них, с одной стороны, часто ведутся разговоры на конфиденциальные темы, а с другой — эти помещения посещают не только сотрудники организации, но и посторонние лица.

Сущность поиска закладки путем визуального осмотра состоит в тщательном осмотре помещения, предметов мебели (книжного шкафа и полок, столов, стульев, кресел, дивана, и др.), компьютера, радио- и электробытовых устройств, телефонных аппаратов, устройств громкоговорящей и диспетчерской связи, картин на стенах, портьер и жалюзи, других предметов в помещении, в которых в принципе можно спрятать малогабаритное закладное устройство. Осмотр проводится без разборки рассматриваемого предмета.

В целях обеспечения полноты визуального контроля целесообразно проводить его по определенной схеме, аналогичной схеме осмотра места происшествия криминалистами: от двери по или против часовой стрелки от периферии к центру помещения. Во время осмотра обращается внимание на свежие царапины на обоях, возле сетевых и телефонных розеток и выключателей освещения, на стенах, винтах корпуса телефонного аппарата, на пылевые следы смещения картины или других предметов, на отрезки проводов и на другие следы или непонятные на первый взгляд предметы.

Для визуального осмотра для поиска закладных устройств применяют различное вспомогательное оборудования. Это оборудование позволяет повысить вероятность обнаружения закладки в ходе визуального осмотра помещения. К такому оборудованию относятся фонари, досмотровые зеркала и технические эндоскопы.

Фонари применяются для осмотра плохо освещаемых мест. Для решения этой задачи могут использоваться малогабаритные бытовые фонари. Но более удобными являются фонари с улучшенными световыми характеристиками.

Досмотровые зеркала применяются для осмотра труднодоступных мест (мебельных ниш, вентиляционных отверстий, под шкафом, диваном и т. д.). Досмотровой комплект зеркал «Шмель-2» включает в себя 2 сменных зеркала различных размеров и конфигурации, телескопическую штангу из 5 колен суммарной длиной 1550 мм и фонарь подсветки.

Зеркала «CEM и CEM/ILL» устанавливаются на телескопической рукоятке из 6 секций длиной 140 см в развернутом и 35 см в закрытом состояниях. Шнур на конце рукоятки позволяет варьировать угол обзора. На рукоятке закрепляется фонарь. Вес досмотрового зеркала без фонаря — 519 г, с фонарем — в 2 раза больше.

Для поиска малогабаритных закладок в местах, не просматриваемых с помощью зеркал, можно применять волоконно-оптические технические эндоскопы, которые используются для наблюдения трудно доступных мест.

Эффективность визуального осмотра повышается при контроле труднодоступных мест с помощью индикаторов поля. Для обеспечения излучения радиозакладки с акустоавтоматом во время проверки необходимо включить радиоприемник, телевизор или громко разговаривать.

Визуальный оперативный осмотр кабинета руководителя организации перед началом или после завершения рабочего дня целесообразно поручить его секретарю, так как он (она) может выявить наиболее быстро новые предметы, появившиеся в кабинете, вплоть до появления новой авторучки на столе. Если проверка проводится вечером, то кабинет должен быть закрыт на ночь, а запасные ключи находиться под наблюдением охраны.

Периодический контроль предусматривает углубленную проверку помещения на наличие в нем всех видов закладок. По решаемым задачам периодический контроль должен обеспечивать обнаружение и локализацию закладных устройств, которые не могут быть выявлены во время визуального осмотра. К таким закладкам относятся камуфлированные и малогабаритные некамуфлированные закладки, в том числе закладки, передающие сигналы по про-

водам. Периодичность такой чистки устанавливает руководитель исходя из ценности защищаемой информации, которая зависит как от вида деятельности, так и этапа работы. В типовом варианте периодический контроль может проводиться несколько раз в месяц, а также после каждого ремонта с привлечением посторонних лиц, за работой которых трудно организовать постоянное наблюдение. Набор технических средств, используемых при таком контроле, определяется возможностью организации по их приобретению.

Одной из важнейших задач службы безопасности при подготовке к ответственному совещанию является проверка помещения, в котором оно должно проводиться. Необходимость такой проверки вызвана потенциальной возможностью определения конкурентом или злоумышленником времени и тематики совещания и проведения ими операции по установке в комнате совещания закладного устройства, в том числе дистанционно управляемого.

Глубина «чистки» комнаты совещания зависит от характера использования этого помещения в процессе функционирования организации. Если организация выделяет специальное помещение для проведения совещаний, которое постоянно закрыто на ключ, опечатано печатью ответственного лица, сдается ежесуточно под охрану с соответствующей записью в журнале, то контроль помещения перед совещанием проводится путем визуального осмотра с использованием средств анализа излучений. Если совещание проводится в служебном помещении (кабинете руководителя или его заместителей, в рабочих комнатах сотрудников), то объем проверок соответствует объему периодической «чистки».

Кроме того, нельзя исключить возможность проноса закладки одним из участников совещания. Поэтому эфир возле выделенного помещения целесообразно контролировать и в ходе совещания с помощью автоматизированных комплексов радиомониторинга.

Проведение капитального ремонта помещения связано с угрозой установки в конструктивных или специально созданных пустотах в стенах (для проводов скрытой электропроводки, выключателей и розеток электропитания, вывода проводов для подключения люстры и др.). Постоянно контролировать работников, проводящих ремонт, практически невозможно. Поэтому после капитального ремонта необходимо провести тщательный технический

контроль пустого (до размещения мебели и приборов) помещения на отсутствие в нем закладных устройств. Целесообразно мебель и приборы, находящиеся в кабинете, на время ремонта вынести в другое закрываемое и опечатываемое помещение. Если мебель и приборы оставлены в ремонтируемом помещении или вынесены в незакрываемое помещение или в коридор, то проверяется каждый предмет.

Достоверное обнаружение закладок возможно при комплексном применении аппаратуры, выявляющей прямые и косвенные демаскирующие признаки: радиоизлучения, пустоты в стене, металлические и нелинейные элементы. Учитывая высокую стоимость набора такой аппаратуры и сравнительно малую частоту проведения подобного ремонта, для проверки помещения после ремонта целесообразно привлекать специализированные организации.

Обнаруженные закладные устройства изымаются или оставляются на месте для передачи дезинформации. Если изъятие выявленной закладки связано с необходимостью проведения достаточно серьезных строительных работ, то закладки, подключенные к телефонной линии или цепям электропитания, дешевле «сжечь» высоковольтными импульсами, отсоединив от проверяемой линии все радиоэлектронные средства. Кроме того, провода телефонной линии необходимо отсоединить от распределительной коробки.

Распознавание обнаруженных предметов с подозрением на закладку, а также проверку представительских и других подарков или изделий, приобретаемых по предварительному заказу или с доставкой к месту эксплуатации фирмой посредником, проводится:

- путем механической разборки, если таковая допускается по условиям эксплуатации или не предполагается дальнейшее использование обнаруженного предмета;
- просвечиванием рентгеновскими лучами неразбираемых предметов;
- облучением полем нелинейного локатора предметов, которые по своему прямому функциональному назначению не могут содержать полупроводниковые элементы;
- проведением специальных исследований радиоэлектронной аппаратуры, прежде всего ПЭВМ.

Распознать обнаруженный предмет непонятного по внешнему виду назначения, а не просто его выбросить, важно потому, что факт обнаружения закладки представляет ценную информацию об активных действиях злоумышленника и перехода угроз безопасности информации из состояния потенциальных в состояние реальных.

Различного рода подарки исследуются без нарушения их товарного вида, что возможно путем выявления излучений, дистанционного обнаружения полупроводниковых элементов или просвечивания подарка.

Специальные исследования могут проводиться специалистами при наличии соответствующей аппаратуры. Если не удается выявить закладку по излучаемому ею сигналу, то производится неразрушающая разборка исследуемого средства и анализ каждого из его узлов. Внешними признаками наличия закладки могут быть:

- отличия в технологии монтажа одной из деталей;
- различия в составе и размещении деталей исследуемого узла и идентичного узла другого проверенного средства.

Так как производство современной радиоэлектронной и вычислительной техники основывается на высоких технологиях, требования которых трудно выполнить на неспециализированном предприятии, то нарушения технологии могут быть выявлены специалистами в процессе внешнего осмотра. Например, установка на печатной плате средства закладки в виде микросхемы или камуфлированной детали потребует изменения топологии или монтажа платы, восстановления ее защитного покрытия, что трудно сделать без появления заметной границы слоя лака, разрушенного при пайке.

В случае отсутствия заметных нарушений технологии монтажа надежное выявление посторонних элементов обеспечивает сравнение исследуемого узла или блока с эталоном. В качестве эталона применяют аналогичные узлы других изделий, например, соответствующей платы средства такого же типа. Этот метод связан с дополнительными затратами на приобретение идентичных средств по другим торговым каналам. Поэтому целесообразно при оснащении организации техникой приобретать однотипные средства у разных продавцов с последующим их сравнением. Наиболее

трудоемким представляется процесс выявления закладок на основе технической документации исследуемого средства, получение которой может представлять достаточно сложную задачу.

Разнообразие технических средств обнаружения и локализации закладных устройств ставит перед службой безопасности организации проблему их выбора при покупке и эффективной эксплуатации.

Выбор рационального состава средств для «чистки» помещений определяется:

- ценностью защищаемой информации в выделенных помещениях;
- количеством выделенных помещений;
- периодичностью проведения совещаний и других мероприятий с циркуляцией защищаемой информации;
- финансовым состоянием организации.

Возможно большое количество вариантов набора средств, приобретаемых организацией для «чистки помещения». Рациональный выбор предусматривает такой состав средств, приобретение которых окупается в течение определенного времени (например, до 5 лет) по отношению к затратам на «чистку» помещений с использованием арендованных средств или привлечения специализированных организаций.

Состав средств для обнаружения закладных устройств в общем случае целесообразно разделить на три варианта: минимальный, средний и максимальный.

**Минимальный набор** включает:

- фонарь для освещения темных мест при визуальном поиске;
- индикатор поля;
- сканирующий портативный приемник;
- управляющую программу;
- компьютер, установленный в контролируемом помещении;
- анализатор проводных линий;
- ручной металлодетектор.

Такой набор обеспечивает:

- визуальный осмотр помещений с освещением и контролем уровня электромагнитного поля в труднодоступных местах;
- обнаружение сканирующим приемником излучений закладок с локализацией мест их установки с помощью индикатора поля;

- обнаружение неизлучающих закладок в не содержащих металл местах (кирпичных стенах, предметах мебели, шкафах и т. д.).

Учитывая, что в выделенных помещениях обычно устанавливаются ПЭВМ, целесообразно сопрячь ее со сканирующим приемником и, используя соответствующее программное обеспечение, производить автоматизированный анализ радиообстановки в помещении. В этом случае достигается более высокая вероятность обнаружения радиозакладных устройств.

Но такой набор не обеспечивает надежного выявления закладных устройств, прежде всего закладок дистанционно управляемых, подключенных к электросети или размещаемых в пустотах железобетонных стен.

**Средний набор содержит**:

- электрический фонарь;
- досмотровой комплект зеркал;
- индикатор поля — частотомер;
- автоматизированный комплекс радиомониторинга помещения;
- нелинейный локатор;
- анализатор проводных линий;
- ручной металлодетектор;
- генератор помех в радиодиапазоне.

Такой состав обеспечивает более высокую вероятность обнаружения закладных устройств по сравнению с возможностью предыдущего варианта (за счет радиомониторинга помещения).

В комплект **максимального набора**, кроме указанных для среднего варианта, целесообразно включить технический эндоскоп и рентгенотелевизионную установку. Просвечивание обнаруженных предметов неизвестного назначения из-за высокой стоимости рентгеновских установок и редкости таких событий можно проводить в специализированных организациях или взятым в аренду аппаратом. Однако иметь в организации собственную рентгеновскую установку полезно не только для распознавания закладных устройств, но и для просвечивания корреспонденции, посылок или других предметов неизвестного происхождения и назначения с целью выявления взрывчатых веществ.

## Вопросы для самопроверки

1. Средства, применяемые для звукоизоляции помещения.
2. Средства, применяемые для повышения звукоизоляции дверей и окон.
3. Требования к характеристикам экранов акустических сигналов.
4. Особенности прозрачных кабин.
5. Виды глушителей звука. Какую информацию защищают глушители звука?
6. Особенности звукопоглощающих материалов. Виды звукопоглотителей.
7. Классификация средств обнаружения, локализации и подавления закладных устройств.
8. Виды средств, используемых для обнаружения радиоизлучающих закладных устройств. Преимущества и недостатки индикаторов поля.
9. Типовой состав автоматизированных комплексов радиомониторинга.
10. Типы аппаратуры контроля проводных линий.
11. Принципы работы обнаружителей пустот.
12. Особенности нелинейных локаторов. Типы нелинейных локаторов.
13. Виды и типы рентгеновских аппаратов.
14. Принципы работы параметрических и индукционных металлодетекторов.
15. Типы средств, нарушающих работу закладных устройств.
16. Типовой состав средств для обнаружения закладных устройств.

# Глава 24. Средства предотвращения утечки информации через ПЭМИН

Средства защиты информации от утечки через побочные электромагнитные излучения и наводки должны удовлетворять следующим требованиям:

а) Опасные сигналы, которые могут содержать конфиденциальную информацию, должны быть ослаблены до уровня, исключающего съем с них информации на границе контролируемой зоны. Учитывая, что чувствительность современных приемников составляет доли мкВ, то уровень опасных сигналов на входе приемника, расположенного на границе контролируемой зоны, не должен превышать эти значения. Если уровни опасных сигналов на выходе создающих их устройств, например акустоэлектрических преобразователей, составляют единицы и десятки мВ, то средства защиты должны обеспечить ослабление амплитуд опасных сигналов на 100–120 дБ.

б) Средства защиты не должны вносить заметных искажений в работу функциональных устройств, используемых сотрудниками организации, и усложнять процесс пользования ими.

Поскольку опасные сигналы являются побочным продуктом работы различных радиоэлектронных средств и возникают случайным образом, а к их источникам, как правило, отсутствует прямой доступ (без нарушения конструкции), то возможности применения способов технического закрытия или шифрования речи в этих электромагнитных каналах утечки отсутствуют. Основной способ защиты информации в них — энергетическое скрытие.

## 24.1. Средства подавления опасных сигналов акустоэлектрических преобразователей

Средства подавления опасных сигналов размещаются в радиоэлектронном средстве или чаще включаются между защищаемым средством и проводами соответствующих информационных линий. Простейшим устройством отключения от линии является выключатель (тумблер), дополнительно устанавливаемый на телефонном аппарате. Более сложные устройства отключения содержат электромагнитные реле, которые подключают телефонный

аппарат только при поднятии трубки или поступлении на аппарат с положенной трубкой сигнала вызова от другого абонента.

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов устаревшей (с электромеханическим звонком) конструкции (рис. 24.1). Емкость конденсатора выбирается такой величины, чтобы зашунтировать опасные сигналы, возникающие в обмотке катушки якоря звонковой цепи в результате воздействия на якорь акустических волн в звуковом диапазоне частот. Этот конденсатор оказывает на сигналы вызова частотой 25 Гц слабое влияние, так как частоты речевого сигнала значительно выше.

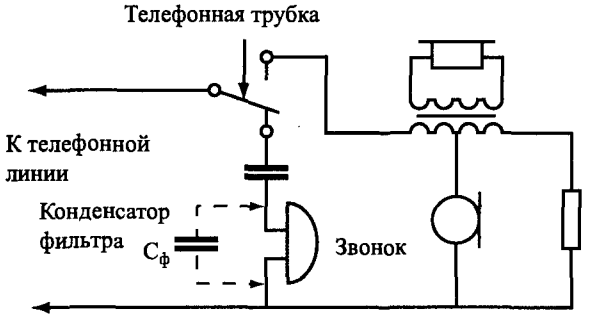



*Рис. 24.1.* Фильтрация опасного сигнала в звонковой цепи

Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах, подавляющий более высокие частоты акустоэлектрических преобразователей по сравнению с полезными сигналами часов единого времени, охранных и пожарных извещателей и др. Двухзвенный П-образный фильтр обеспечивает затухание опасных сигналов, возникающих во вторичных часах за счет акустоэлектрических преобразований, примерно на 85 дБ. Подобные фильтры обеспечивают защиту информации в телефонных аппаратах от высокочастотного навязывания, не пропуская к ним высокочастотные электрические сигналы от генератора, подключенного злоумышленником к соответствующей телефонной линии. Полезные сигналы в речевом диапазоне частот проходят через фильтр без заметного ослабления.

Возможность ограничения опасных сигналов основывается на нелинейных свойствах полупроводниковых элементов (ди-

одов, транзисторов, динисторов, тиристоров). Вольтамперная характеристика (зависимость значения протекающего по нелинейному элементу электрического тока от приложенного к нему напряжения источника тока) полупроводникового диода показана на рис. 24.2.

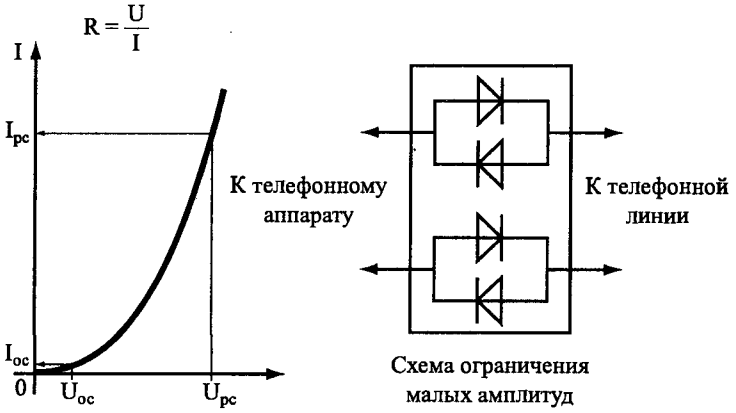



*Рис. 24.2.* Принципы ограничения малых амплитуд

Так как сопротивление диода согласно закону Ома равно отношению значения напряжения на его выводах к величине протекающего по диоду тока, то из этого рисунка следует, что диод создает высокое (сотни тысяч ом) сопротивление для сигналов с низким (доли и единицы мВ) напряжением и малое (сотни Ом) — для полезных сигналов в телефонных линиях величиной в десятки вольт. Поэтому опасные сигналы, возникающие в защищаемых радиоэлектронных средствах и имеющие малую амплитуду по сравнению с полезным сигналом, дополнительно ослабляются в тысячи раз, а полезные сигналы проходят через полупроводниковый ограничитель практически без затухания. Например, устройство «Гранит-VIII» обеспечивает ослабление входного сигнала амплитудой не более 0,1 около 65 дБ, а сигнала амплитудой более 10 В всего на 3 дБ В. Рассмотренный способ защиты информации реализован в устройствах «Корунд», «Гранит-VIII МП-1», МП-1 (для аналоговых ТА), МП-1ЦА (для цифровых ТА с автономным питанием), МП-1ЦЛ (для цифровых ТА с питанием от мини-АТС).

Сочетание фильтра и ограничителя широко используется в устройствах комплексной защиты информации путем подавления

опасных побочных сигналов и сигналов высокочастотного навязывания (Грань-300, МП-1А и др.).

Для подавления опасных сигналов, возникающих в громкоговорителях, рассмотренные средства защиты не применяются в силу несущественных отличий признаков полезных и опасных сигналов. Действительно, частоты их совпадают — звуковой диапазон. Так как катушка динамической головки громкоговорителя имеет малое сопротивление порядка 4–8 Ом, то для исключения перегорания ее тонкого провода величина напряжения сигнала, подаваемого на катушку невелика, доли В. С этой целью сигнал ретрансляционной сети, имеющий для сети города напряжение 15 В, а области 30 В, подается на громкоговоритель через понижающий трансформатор. В результате этого соотношение уровней опасного и полезного сигналов в катушке громкоговорителя недостаточное для эффективного использования ограничителей малых амплитуд. Поэтому для подавления опасных сигналов громкоговорителя применяют устройство, отличающее опасные сигналы от полезных по их направлению. Таким устройством является буферное устройство в виде одного или нескольких последовательно соединенных эмиттерных повторителей. Эмиттерный повторитель представляет собой каскад усилителя мощности с общим эмиттером (см. рис. 24.3), у которого коэффициент усиления сигнала по напряжению близок к 1.

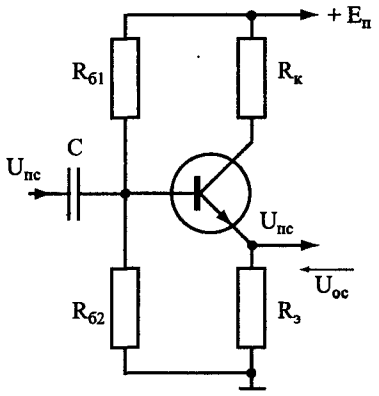



*Рис. 24.3.* Эмиттерный повторитель буферного устройства

Эмиттерный повторитель имеет высокое входное и малое выходное сопротивления и применяется для согласования взаимо-

действующих радиотехнических устройств с существенно отличающимися выходными и входными сопротивлениями.

Полезный сигнал $U_{пс}$ извне проходит к громкоговорителю через эмиттерный повторитель без заметных изменений, а внутренний опасный сигнал $U_{ос}$ подавляется до 1000 раз (60 дБ по напряжению). Учитывая высокий уровень опасного сигнала громкоговорителя, для его гарантированного подавления в буферном устройстве соединяют последовательно 3 эмиттерных повторителя с общим коэффициентом подавления до 180 дБ.

## 24.2. Средства экранирования электромагнитных полей

Для экранирования электромагнитных полей применяются специальные конструкции и разнообразные материалы. Специальные конструкции включают экранированные сооружения, помещения и камеры. Они могут быть стационарными, сборно-разборными и мобильными. Выполняются из стальных листов толщиной 2–3 мм и обеспечивают затухание электромагнитного поля 60–120 дБ. Для обеспечения нормальной работы они оборудуются защищенными дверьми, воротами, проемами с устройствами сигнализации о плотном закрытии, разнообразными помехоподавляющими фильтрами, средствами вентиляции и кондиционирования, пожарной сигнализации, пожаротушения и дымоулавливания.

В качестве материалов для эффективного экранирования используются **металлические листы и сетки**. Стальные листы толщиной 2–3 мм, сваренные герметичным швом, обеспечивают наибольший экранирующий эффект (до 100 и более дБ). Толщина стального листа выбирается исходя из прочности конструкции и возможности создания сплошного шва. При сварке переменным током толщина сплошного шва обеспечивается при толщине листов 1,5–2 мм, на постоянном токе — около 1 мм, газовая сварка позволяет создать сплошной шов при толщине свариваемых листов до 0,8 мм.

Однако металлические листы имеют высокую цену, а изготовление из них экранов и их эксплуатация требуют больших затрат. Коррозия и появляющаяся во время монтажа напряженность сварочных швов снижают надежность и долговечность экранов, а не-

обходимость их периодической проверки и устранения дефектов повышают эксплуатационные расходы.

Более дешевые и удобные, но менее эффективные экраны из **металлической сетки**. Применяют для экранирования сетки из луженой стальной и латунной проволоки с ячейками размерами от долей (0,25) мм до единиц (3–6) мм. Экранирующие свойства сетки в основном определяются отражением электромагнитной волны от ее поверхности. Эффективность экрана из луженой низкоуглеродистой стальной сетки с ячейками размером 2,5–3 мм составляет на частотах Гц 55–60 дБ, а из двойной сетки с расстоянием между слоями 100 мм достигает эффективности экранов из стальных листов — около 90 дБ. По соотношению радиуса r проволоки сетки и шага сетки s различают густые и редкие сетки. К густым относятся сетки, у которых $s/r \le 8$, у редких — $s/r > 8$. Эффективность экранирования редкой сетки определяется по формуле:

$$S_c = \frac{\lambda}{2s\left[\ln\left(2\pi r / s\right)\right]}.$$

Для густых сеток более точный результат получается при замене величины $\ln(2\pi r/s)$ в этой формуле на $2\pi r/s$.

Наряду с рассмотренными традиционнымн средствами для электромагнитного экранирования в последнее время все шире применяются **фольговые** и **металлизированные материалы, токопроводящие краски** и **клеи, радиопоглощающие строительные материалы**.

В качестве **фольговых материалов** используются фольга толщиной 0,01–0,08 мм, наклеиваемая на экранируемую поверхность, и фольга на непроводящей подложке, например на фольгоизоле. Фольга изготовляется из алюминия, латуни, цинка.

**Металлизация** различных материалов применяется для электромагнитного экранирования благодаря универсальности метода распыления расплавленного металла струей сжатого воздуха. Движущиеся с большой скоростью распыленные частицы металла ударяются о поверхность подложки, деформируются и соприкасаются друг с другом. При этом обеспечивается прочная связь с подложкой и непрерывная проводимость покрытия. Этот метод позволяет нанести металлический слой практически на любую по-

верхность: плотную бумагу, ткань, дерево, стекло, пластмассу, бетон и др. Толщина наносимого слоя зависит от физико-химических свойств подложки. Для плотной бумаги слой металла характеризуется величиной не более 0,28 кг/м$^2$, для ткани — 0,3 кг/м$^2$, для жесткой подложки толщина не ограничивается. В качестве металла покрытия чаще используется цинк, реже алюминий. Алюминиевое покрытие имеет более высокий (примерно не 20 дБ) коэффициент экранирования, но оно менее технологично.

Эффективность экранирования металлизированной цинком поверхности оценивается по эмпирической формуле:

$$S_{мет} = 97 + 5\lg d_0 - 20\lg f,$$

где $d_0$ — количество распыленного металла, кг/м$^2$, f — частота поля, Мгц.

Из металлизированных материалов наиболее широко применяются **металлизированные ткани** и **пленки (стекла)**. Ткани металлизируются как путем вплетения в нее металлизированных или металлических нитей пряжи, так и путем нанесения на поверхность ткани слоя металла. При этом у тканей сохраняются не только ее первоначальные свойства (гибкость, воздухопроницаемость, легкость) и внешний вид, но появляются дополнительные стойкость к агрессивным средам и противопожарная устойчивость. Ткань можно сшивать, склеивать и даже паять. Эффективность экранирования металлизированных тканей в высокочастотном диапазоне (сотни МГц) достигает 50–70 дБ. Их применяют для экранирования стен и оконных проемов (в виде штор), корпусов продукции, антенных отражателей, чехлов на объекты радиолокационного наблюдения.

Электрические и оптические свойства стекол с токопроводящим покрытием зависят от состава токопроводящей пленки, ее толщины, методов ее нанесения и свойств стекла. Допустимые снижение прозрачности пленки не более 20% и электропроводность обеспечиваются при толщине пленки 5–3000 нм. Наибольшее распространение получили пленки из окиси олова.

Стекла с токопроводящими покрытиями имеют поверхностное электрическое сопротивление порядка 5–10 Ом при незначитель-

ном (не более 20%) ухудшении прозрачности. **Токопроводящие пленки**, наклеиваемые на стекла окон, позволяют повысить экранирующий эффект окон без ухудшения их внешнего вида и прозрачности на 18–22 дБ на частотах в сотни МГц и на 35–40 дБ на частотах единицы ГГц. В зависимости от вида напыляемого на пленку металла они имеют золотистый (медное напыление) или серебристый (алюминиевое напыление) цвет.

**Токопроводящие краски** создаются путем ввода в краски токопроводящих материалов: коллоидного серебра, графита, сажи, оксидов металла, порошковой меди и алюминия и других металлов. Наилучшие результаты обеспечивает краска, у которой в качестве токопроводящего пигмента применяется ацетиленовая сажа и графит. Например, краска, представляющая композицию лака 9-32 и 300% карандашного графита, имеет поверхностное сопротивление 7–7,6 Ома при толщине покрытия 0,15–0,17 мм и сопротивление 5–6 Ом при толщине покрытия 0,2–0,21 мм.

Токопроводящие краски в силу худшей электропроводности и малой толщины обеспечивают меньшую по сравнению с металлизированными тканями экранирующую эффективность, но не менее 30 дБ в широком диапазоне частот. Но из-за простоты нанесения на поверхность эмали широко применяются для:

- экранирования ограждений (стен, потолков, дверей);
- защиты контактных поверхностей от окисления;
- окрашивания внутренней поверхности корпусов аппаратуры;
- проведения профилактических и ремонтных работ, в том числе для заделки щелей, отверстий, выводов труб из стен, для улучшения контакта между металлизированными пленками и металлическими экранами стен.

**Электропроводные клеи** применяются вместо пайки и болтовых соединений элементов электромагнитных экранов, а также для заполнения щелей и малых отверстий в них. Основу электропроводного клея составляет смесь эпоксидной смолы и тонкодисперсных порошков железа, кобальта или никеля. Про прочности до 500 кг/см$^2$ такой клей имеет низкую удельную электропроводность.

Для повышения экранирующей способности потолков, стен, полов помещений применяются **ферритодиэлектрические обли-**

**цовочные материалы**, поглощающие электромагнитные поля. Этот поглотитель представляет собой панель из склеенных металлической подложки, ферритового и диэлектрического материалов. Ферритодиэлектрический поглотитель электромагнитных волн экологически чист, имеет стабильные радиотехнические характеристики в широком диапазоне частот, обеспечивает коэффициент отражения –12–(–40) дБ в диапазоне частот 0,03–40 ГГц, устойчив к воздействию огня.

Путем добавки в бетон строительных конструкций токопроводящих материалов удается также повысить экранирующие свойства стен и перекрытий зданий.

Металлизированные ткани и пленки, фольговый материал, токопроводящие эмали эффективно экранируют слабые побочные электромагнитные излучения и наводки, но их экранирующая способность недостаточна для энергетической скрытности более мощных сигналов, например излучений передатчиков закладных устройств, не говоря уже об излучениях настраиваемых или испытуемых в исследовательских лабораториях создаваемых излучающих радиоэлектронных средств.

Для гарантированного ослабления опасных сигналов при жестких требованиях к уровню безопасности информации источники излучений размещают в экранированных помещениях (экранных комнатах), ограждения которых покрыты стальными листами или металлическими сетками. Размеры экранированного помещения выбирают из его назначения и стоимости экранирования. Существуют экранированные вычислительные центры площадью в многие десятки $м^2$, но обычно экранные комнаты для проведения измерений радиоизлучающих блоков и антенн имеют небольшую площадь в 6–8 $м^2$ при высоте 2,5–3 м. Металлические листы или полотнища сетки, покрывающие стены, потолок и пол, должны быть прочно, с малым электрическим сопротивлением, соединены между собой по периметру. Для сплошных экранов это соединение обеспечивается сваркой или пайкой, для сетчатых экранов должен быть обеспечен точечной сваркой или пайкой хороший электрический контакт между полотнищами не реже чем через 10–15 мм.

Двери должны быть также экранированы. При их закрывании необходимо обеспечить надежный электрический контакт с металлическими листами или сеткой стен по всему периметру дверей. Для этого применяют пружинную гребенку из фосфористой бронзы, которую укрепляют по внутреннему периметру дверной рамы.

При наличии в экранной комнате окон последние должны быть затянуты одним или двумя слоями сетки, расстояние между слоями двойной сетки не менее 50 см. Слои сетки должны иметь хороший электрический контакт с экраном стен по всему периметру оконной рамы. Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой размером 2,5–3 мм, уменьшает уровень излучений на 55–60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) приблизительно на 90 дБ. Сетки для обеспечения возможности мытья стекол удобнее делать съемными, а металлическое обрамление съемной части должно иметь пружинящие контакты в виде гребенки из фосфористой бронзы.

При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нормальные условия для работающего в нем человека, прежде всего, вентиляцию воздуха и освещение. Это тем более важно, так как у человека в экранной комнате может ухудшиться самочувствие из-за экранирования магнитного поля Земли.

Для эффективного электромагнитного экранирования вентиляционные отверстия на частотах менее 1000 МГц закрывают сотовыми экранами с прямоугольными, круглыми, шестигранными ячейками. Для обеспечения эффективного электромагнитного экранирования необходимо, чтобы размеры ячеек экрана не превышали 0,1 длины волны поля. Но на высоких частотах размеры ячеек могут быть столь малыми, что ухудшится вентиляция через них воздуха. Поэтому на частотах выше 1000 МГц применяют специальные электромагнитные ловушки в виде конструкции из поглощающих электромагнитные поля материалов, вставляемой в вентиляционные отверстия.

Величины затухания радиосигнала в экранированном помещения в зависимости от конструкции экрана указаны в табл. 24.1.

*Таблица 24.1*

| *Тип конструкции экрана* | *Затухание радиосигнала, дБ* |
|---|---|
| Одиночный экран из сетки с одиночной дверью, оборудованной зажимными устройствами | 40 |
| Двойной экран из сетки с двойной дверью-тамбуром и зажимными устройствами | 80 |
| Сплошной стальной сварной экран с одной дверью-тамбуром с зажимными устройствами | 100 |

## Вопросы для самопроверки

1. Требования к средствам защиты информации от утечки через побочные электромагнитные излучения и наводки.
2. Типы средств для подавления опасных сигналов акустоэлектрических преобразователей.
3. Что представляют собой специальные конструкции для экранирования полей?
4. Какие материалы используются для экранирования электромагнитных полей?
5. Достоинства и недостатки пленок, красок и клея, применяемых для электромагнитного экранирования.

## Основные положения раздела III

1. Силы и средства, обеспечивающие добывание иифорлации в интересах государства или организации, образуют систему разведки. Независимо от решаемых задач и имеющего ресурса система включает три органа: планирования и управления, добывания данных и сведений, а также информациониой работы. Орган планирования и управления получает задание от потребителей информации, разрабатывает замысел и план разведывательной операции, ставит задачи исполнителям (органам добывания) и обеспечивает нормативное и оперативиое управление ими. В ходе планирования орган управления взаимодействует с органом информационной работы. Органы добывания находят объекты разведки, вступают с ними в разведывательные контакты, получают от них данные и передают их в органы сбора и обработки. Органы обработки осу-

ществляют видовую и комплексную обработку собранных данных и сведений. Видовая и комплексная обработка отличаются языками представления информации. При видовой обработке используется в основном язык признаков, комплексная обработка осуществляется на профессиональном языке разведки. В процессе добывания данных и информационной работы может возникнуть необходимость в уточнении и добывания дополнительного данных — в доразведке. Итоговая разведывательная информация через органы управления передается потребителям информации. Возможности системы разведки по добыванию информацию зависят, в основном, от характеристик технических средств добывания и обработки, а также способов доступа средств к источникам информации.

2. Технические средства добывания информации существенно расширяют и дополняют возможности человека, обеспечивая: съем информации с носителей, которые не воспринимаются органами чувств человека; добывание информации без нарушения границ контролируемой зоны; передачу информации практически в реальном масштабе времени в любую точку земного шара; анализ и обработку информации в объеме и за время, недостижимые человеком; консервацию и сколь угодно долгое хранение добываемой информации. Технические средства добывания информации по назначению можно разделить на средства подслушивания, наблюдения, перехвата и физико-химического анализа. Эти средства в зависимости от места установки и условий эксплуатации имеют различные схемотехнические и конструктивные решения. Жесткие требования к масса-габаритным характеристикам, энергопотреблению, устойчивости к механическим воздействиям предъявляются к техническим средствам разведки, устанавливаемым на летательных и космических аппаратах. Наземные средства по условиям эксплуатации делятся на стационарные и мобильные, а мобильные — на возимые и носимые (некамуфлированные и камуфлированные). Средства добывания, камуфлированные под различные бытовые приборы и предметы личного пользования, могут быть максимально приближены и источникам информации, но их технические параметры обычно хуже аналогичных параметров некамуфлированных средств. Все шире применяются автономно работающие и дистанционно управляемые закладные подслушиваю-

щие устройства в помещениях, портативные средства наблюдения, автономные портативные технические средства разведки на местности, устройства слежения за транспортными средствами.

Основными характеристиками технических средств, в наибольшей степени влияющими на их возможности по добыванию информации, являются диапазон частот, чувствительность и разрешающая способность. От чувствительности зависит дальность добывания, а разрешающая способность определяет количество и информативность добываемых признаков об объекте разведки. На возможности технической разведки влияют способы доступа средств добывания к источникам информации. Чем ближе к источнику информации удается разместить средство добывания, тем большее количество информации может быть им добыто. В мирное время к любому объекту разведки на суше и воде могут приблизиться на расстояние 130–150 км разведывательные космические аппараты, на которые устанавливаются средства наблюдения и перехвата радиосигналов. Большинство разведывательных КА имеют низкоорбитальные круговые траектории с различными углами наклона их плоскостей относительно поверхности Земли. Но возможность точного расчета времени и кратковременность пролета низкоорбитальных КА над объектом разведки позволяют обеспечить эффективную временную скрытность его признаков.

3. Основу комплекса средств подслушивания составляет акустический приемник, включающий акустоэлектрический преобразователь, селективный усилитель, громкоговоритель (телефон). Для запоминания акустических сигналов к выходу селективного усилителя подсоединяется аудиомагнитофон, а для технического анализа — средства анализа акустических сигналов. Возможности акустического приемника характеризуются диапазоном частот принимаемого акустического сигнала, чувствительностью, динамическим диапазоном и масса-габаритными характеристиками. Основной элемент акустического приемника — акустоэлектрический преобразователь (микрофон, стетоскоп, акселерометр, гидрофон, стеофон). По принципу действия микофоны делятся на угольные, электродинамические, конденсаторные, электретные и пьезоэлектрические, по направленности — ненаправленные, односторонней, двусторонней и острой направленности. Наибольшую

дальность подслушивания (десятки метров) обеспечивают специальные (параболические, трубчатые, плоские и градиентные) остронаправленные микрофоны. Для увеличения дальности подслушивания применяют ретрансляторы, преобразующие акустический сигнал в радио-, электрические и оптические сигналы, существенно меньше затухающие в среде распространения, чем акустический сигнал.

В качестве ретрансляторов широко используются закладные устройства. Закладные устройства по виду носителя информации бывают проводными (носитель — электрический ток) и излучающими (носитель — электромагнитное поле и свет в инфракрасном диапазоне); по виду первичного сигнала — акустические и аппаратные; по способу установки — с заходом и без захода; по режиму работы — неуправляемые, управляемые акустоавтоматом и дистанционно управляемые; по стабильности частоты сигнала — нестабилизированные, «мягкой» и «жесткой» стабилизацией; по виду электропитания — с автономным питанием, с питанием от сети, от цепей электропитания технического средства, в котором устанавливаются закладные устройства, от внешнего источника радиоизлучений; по способу закрытия — незакрытые и закрытые. Закладные устройства в зависимости от частотного диапазона, мощности сигнала, типа антенны обеспечивают передачу речевой информации на расстояние от десятков до сотен метров. Малые габариты и вес закладных устройств позволяют их встраивать (камуфлировать) в разнообразные средства и бытовые предметы.

При определенных условиях речевая информация в помещениях может быть дистанционно подслушана с помощью лазерных средств и устройств высокочастотного навязывания. Для обеспечения лазерного подслушивания на колеблющееся под действием акустического речевого сигнала в помещении стекло подается от лазерного излучателя луч света в инфракрасном диапазоне. Отраженный луч модулируется по частоте, углу и фазе колебаниями стекла. При приеме и демодуляции этого лазерного луча с него снимается речевая информация. Оперативное применение лазерного подслушивания существенно ограничивает необходимость обеспечения перпендикулярности лазерных лучей к поверхности стекла. Подслушивание с помощью высокочастотного навязы-

вания достигается путем подачи на телефонный аппарат по проводам телефонной линии высокочастотного электрического сигнала или облучения внешним электромагнитным полем пассивного закладного устройства, размещенного в помещении. В первом варианте в нелинейных элементах телефонного аппарата происходит модуляция внешнего сигнала сигналами случайных акустоэлектрических преобразователей этого аппарата и излучение его проводами модулированного сигнала в эфир. Во втором варианте переотраженный закладным устройством внешнее электромагнитное поле модулируется в соответствии с изменяющимися под действием акустического сигнала электрическими параметрами закладного устройства.

Для скрытой записи речевой информации применяют специальные кинематические и бескинематические (цифровые) диктофоны, отличающиеся от диктофонов широкого применения меньшими количеством и информативностью их демаскирующих признаков.

4. В оптическом видимом диапазоне света информация разведкой добывается путем визуального, визуально-оптического, фото-, видео- и киносъемки, телевизионного наблюдения, а в инфракрасном диапазоне — с использованием приборов ночного видения и тепловизоров. Типовой оптический приемник содержит оптическую систему, светочувствительный элемент, усилитель и индикатор. Основными характеристиками оптического приемника являются: диапазон длин волн световых лучей, воспринимаемых средством наблюдения, чувствительность, разрешающая способность, поле (угол) зрения и изображения, динамический диапазон значений силы света на входе приемника. Параметры оптического приемника определяются в основном характеристиками оптической системы и светочувствительного элемента. Основу оптической системы составляют объективы, возможности которых характеризуются искажениями изображения (аберрациями), фокусным расстоянием, углом поля зрения (изображения), светосилой, разрешающей способностью, частотно-контрастной характеристикой. Дальность визуального наблюдения повышается с помощью визуально-оптических приборов (биноклей, монокуляров, подзорных труб, специальных телескопов), изображения объекта наблю-

дения фиксируют пленочные и цифровые фотоаппараты, изображения движущихся объектов наблюдаются с помощью телевизионных средств, а записываются видеомагнитофонами. Для наблюдения через малые отверстия диметром 6–10 мм используются технические эндоскопы.

В качестве светочувствительных элементов применяются в основном черно-белые, цветные и спектрозональные фотоматериалы (фото- и кинофотопленка, фотопластины и фотобумага) и твердотелые приборы (ПЗС-матрицы) с зарядовой связью на МОП-структурах. ПЗС-матрицы в силу прямого преобразования света в электрические заряды, малых габаритов, высоких разрешающей способности и чувствительности составляют основу оптико-электронных средств наблюдения (телевизионных и видеокамер, цифровых фотоаппаратов). В качестве индикаторов оптического приемника применяют фотобумагу, электровакуумные приемные трубки (кинескопы), жидкокристаллические и газоразрядные панели.

Для наблюдения объектов в инфракрасном диапазоне, отражающих свет внешних источников, применяются приборы ночного видения (ПНВ), а для формирования изображений по собственным тепловым излучениям объектов — тепловизоры. Основу ПНВ составляют объектив и электронно-оптические преобразователи 1–4 поколений. Более высокая чувствительность тепловизоров достигается снижением тепловых шумов светоэлектрических преобразователей путем их охлаждения.

В радиодиапазоне наземные объекты наблюдаются с помощью радиолокационных станций. Для повышения разрешающей способности в радиолокационных станциях бокового обзора (РЛС БО), устанавливаемых на летательных и космических аппаратах, увеличивают физические размеры вдольфюзеляжной антенны или виртуальные размеры антенны с синтезированной апертурой. Радиотеплолокационное наблюдение объектов возможно с помощью специальных радиоприемных средств — радиометров.

5. Для перехвата и технического анализа радиосигналов используются комплексы, типовой вариант которых включает антенну, радиоприемник, пеленгатор, анализатор, устройство индикации и регистрации сигналов. Антенны представляют собой электромеханические конструкции из токопроводящих элементов, раз-

меры и конфигурация которых определяют эффективность преобразования радиосигналов в электрические сигналы. Основные параметры антенны: диаграмма направленности и ее ширина, коэффициенты полезного действия, направленного действия, усиления, а также полоса излучаемых (принимаемых) частот. По типу излучающих элементов антенны делятся на линейные, апертурные и поверхностных волн. По конструкции линейные антенны разделяют на симметричные и несимметричные электрические вибраторы, бегущей волны, ромбические и рамочные антенны, а апертурные — на рупорные, линзовые, зеркальные и щелевые антенны.

Радиоприемник комплекса перехвата осуществляет селекцию по частоте определенного сигнала в антенне, его усиление, демодуляцию, усиление видео- или низкочастотного первичного сигнала. Основные характеристики радиоприемника: диапазон принимаемых частот, чувствительность, избирательность, динамический диапазон и уровни искажений. Наибольшие возможности имеют сканирующие радиоприемники, которые отличаются от традиционных электронной перестройкой в очень широком диапазоне частот (от долей МГц до нескольких ГГц), наличием блоков памяти для запоминания частот принимаемых сигналов и интерфейса для сопряжения с компьютером. На основе сканирующих приемников и ПЭВМ создаются автоматизированные комплексы радиоконтроля. Технические средства измерения признаков сигналов включают большой набор различных программно-аппаратных средств и приборов, в том числе устройства панорамного обзора и анализа спектра сигналов, селективные вольтметры, измерители временных параметров дискретных сигналов, определители видов модуляции и кода и других демаскирующих признаков сигналов. Пеленгатор комплекса определяет направление на источник радиоизлучения и его координаты. Точность пеленгования зависит от метода пеленгования, систематических ошибок пеленгатора, погрешностей измерения пеленгов и характера распространения электромагнитных волн от их источника к антенне пеленгатора. Наиболее высокую точность пеленгования обеспечивают фазовые методы при прямом (без переотражения) распространении электромагнитной волны. Регистрация (запись, запоминание) сигналов с добытой информацией производится путем аудио-, видеозаписи на магнитные

ленту и диски, на оптические диски, на обычной, электрохимической, термочувствительной и светочувствительной бумаге, в устройствах полупроводниковой и других видов памяти, фотографирования изображений на экранах мониторов ПЭВМ, телевизионных приемников, осциллографов и спектроанализаторов.

6. Вещественные признаки продукции, содержащие защищаемую информацию, определяются в результате химического, физико-химического и физического анализа. Основу химического анализа составляют химические реакции изучаемого вещества в растворе. Физико-химический анализ предусматривает измерение физических величин, изменение которых обусловлено химическими реакциями. Физический анализ учитывает изменение физических характеристик добытой пробы, вызванных исследуемым веществом. Принципы и методы определения химического состава вещества рассматривает аналитическая химия, которая включает качественные и количественные методы анализа. Для аналитической химии характерно применение не только традиционных химических методов, но и физико-химических и физических методов, а также биологических методов. Основными методами аналитической химии являются методы разделения веществ, термические, химические, электрохимические, хроматографические методы, спектральный анализ, масс- спектрографические, радиоактивные и биологические методы. Если количество добытого вещества очень мало (порядка 100 мкг), то используются методы микрохимического анализа, при меньшем количестве (единицы и доли мкг) — методы ультрамикрохимического анализа.

Для обнаружения и измерения радиоактивных излучений используют фотографический, сцинтилляционный, химический и ионизационный методы. Наиболее широко применяются ионизационные и сцинтилляционные методы обнаружения радиоактивного излучения. Структура типового прибора радиационной разведки содержит детектор, усилитель, индикатор и блок питания. В качестве детекторов, преобразующих энергию радиоактивного излучения в электрические сигналы, используются ионизационные камеры, газоразрядные счетчики, кристаллы полупроводника. Приборы для обнаружения и измерения радиоактивных излучений делятся на индикаторы радиоактивности, измерители мощности дозы (радиометры) и дозиметры.

7. Система инженерно-технической защиты информации состоит из подсистемы физической защиты информации, подсистемы защиты информации от утечки и комплекса управления силами и средствами инженерно-технической защиты информации. Средства подсистемы физической защиты источников информации должны обнаруживать и задерживать источники угроз на время, превышающее время, необходимое для их нейтрализации. Эти средства образуют комплексы инженерной защиты и технической охраны. Основу комплекса инженерной защиты составляют: инженерные конструкции на рубежах защиты и отдельных направлениях, средства контроля и управления допуском в контролируемые зоны людей и транспорта. Комплекс технической охраны источников информации объединяет силы и средства обнаружения и наблюдения за источниками угроз, а также силы и средства их нейтрализации.

Силы и средства подсистемы защиты информации от утечки противодействуют несанкционированному распространению носителей с защищаемой информацией от их источников к злоумышленнику. Их можно разделить на комплексы средств защиты информации от наблюдения, подслушивания, перехвата и противодействия утечке вещественных носителей информации. Управление силами и средствами системы инженерно-технической защиты информации обеспечивает комплекс управления.

8. Средства инженерной защиты объединяют конструкции, затрудняющие движение злоумышленника и распространение стихийной силы к источнику информации, и включают ограждения (заборы, двери и ворота, окна, стены зданий, стены, потолок и пол помещений), шкафы, сейфы и хранилища, а также средства контроля и управления доступом людей и транспорта в контролируемые зоны. По назначению ограждения делятся на основные, дополнительные и вспомогательные. Основным ограждением территории организации является забор. Заборы делятся на декоративные и защитные. Защитные заборы бывают монолитными, сборными бетонными или железобетонными, металлическими (литыми, коваными, сварными), сетчатыми, проволочными, деревянными, растительными (в виде живой изгороди) и комбинированными. Высота капитальных заборов может достигать 2,5 м. Капитальные

кирпичные и бетонные заборы укрепляются установкой сверху дополнительных проволочных ограждений в виде 3–4 ниток армированной колючей ленты, острых стержней или даже битого стекла. Для размещения средств периметровой сигнализации, телевизионного наблюдения, связи, освещения, тропы движения сотрудников охраны и собак, а также постовых укрытий между основным и предупредительным заборами создается зона отторжения. Если в зоне отторжения устанавливаются технические средства охраны периметра, то ширина зоны отторжения устанавливается не менее ширины их зоны обнаружения. Для обнаружения прохода злоумышленника через зону отторжения она может оборудоваться контрольно-следственной полосой из взрыхленного грунта шириной не менее 1,5 м.

Двери и ворота — традиционные конструкции для санкционированного пропуска людей и транспорта. Прочность дверей характеризуется устойчивостью к взлому, пулестойкостью, устойчивостью к взрыву. Различают двери с нормальной, повышенной и высокой устойчивостью. По устойчивости к взлому двери делятся на 1–5 классы. Классу 5 соответствуют двери, выдерживающие воздействие электрического инструмента режущего и/или ударного действия повышенной мощности, а также термического режущего инструмента и/или сварочного оборудования. Прочность дверей повышается путем: изменения направления открывания двери с «от себя» «на себя»; изготовления дверного полотна из цельных лесоматериалов крепких пород деревьев; установления с обеих сторон дверного полотна стальных полос, стягиваемых болтами; обивки дверных деревянных полотен металлическими листами; укрепления дверной коробки стальными уголками в местах крепления петел и запорных планок замков; «прибития» дверной коробки к проему стены с помощью стальных штырей; установки перед дверью, открываемой наружу, стальной планки, закрываемой дополнительным замком; установки параллельно двери распашной или раздвижной стальной решетки, закрываемой дополнительным замком. Надежность дверей зависит также от взломостойкости замков. Взломостойкость замков определяется его конструкцией, типом металла и секретностью запорного механизма, оцениваемого количеством положений штифтов или кодовых комбина-

ций. По способу закрытия (открытия) замки делятся на механические и электроуправляемые. В зависимости от механизма обеспечения секретности различают бессувальдные, сувальдные, цилиндрические, кодовые и электронные замки. По стойкости к вскрытию замки для дверей делятся на 4 класса.

Традиционно окна укрепляются металлическими решетками. Более современный путь укрепления окон — защитное остекление с использованием закаленных, армированных, ламинированных, многослойных, органических стекол, стеклопакетов и стеклянных пустотелых блоков. Защитное остекление по прочности от брошенного предмета разделяются на классы А1–А3, по защите от пробивания топором Б1-Б3, по устойчивости к воздействию пуль стрелкового оружия — С1–С5.

Для хранения особо ценных документов, вещей, денег применяются сейфы и хранилища. По конструктивному исполнению хранилища могут быть монолитными, сборными и сборно-монолитными. Стойкость хранилищ и сейфов оценивается временем взлома с учетом коэффициента мощности применяемого инструмента. По стойкости хранилища делятся на 13 классов, сейфы — на 10 классов. Сейфы оцениваются также по пожаро- и влагоустойчивости.

9. Уязвимым элементом инженерной защиты является система контроля управления доступом (СКУД) людей и транспорта в различные контролируемые зоны. Эта уязвимость характеризуется вероятностями ложного допуска людей и транспортных средств и ложной задержки (ошибок 1-го и 2-го родов соответственно). На эффективность управления доступом влияет, прежде всего, надежность идентификации людей и транспорта.

Для идентификации применяются атрибутные и биометрические идентификаторы. В качестве атрибутных идентификаторов используются автономные носители признаков допуска: ключи, жетоны, пропуска, удостоверения личности, идентификационные карточки, в которых именные признаки записываются на магнитной полоске, в штрих-коде, в структуре переизлучающих элементов (в карточках «Виганда»), в кодовой последовательности электрического или радиосигнала (в «проксимити» карточках). Современные идентификационные карточки обеспечивают малые ошибки иден-

тификации, но могут попасть к злоумышленнику. Проблема исключения подделки и кражи идентификаторов решается путем применения именных признаков человека — биометрических идентификаторов: отпечатков пальцев, рисунка радужной оболочки глаза и кровеносных сосудов его сетчатки, теплового изображения лица, геометрии кисти руки, динамики подписи, спектральных характеристик речи.

В качестве исполнительных устройств СКУД (управляемых преграждающих устройств) применяются двери, ворота, раздвижные и вращающиеся трех- или четырехштанговые турникеты, шлюзовые тамбуры.

10. Ядро подсистемы охраны источников информации и других ценных объектов составляют средства обнаружения злоумышленника и пожара — извещатели. Извещатели используются для блокирования отдельных объектов, закрытых помещений, открытых пространств, блокирования периметров и обнаружения пожара. По принципу обнаружения извещатели делятся на контактные, акустические, оптико-электронные, микроволновые, вибрационные, емкостные, тепловые, ионизационные и комбинированные, по виду обнаружения — точечные, линейные, поверхностные и объемные. Эффективность работы извещателя оценивается вероятностями правильного и ложного обнаружения злоумышленника или пожара. Для увеличения вероятности обнаружения и снижения ложных срабатываний извещателей от помех увеличивают количество добываемых ими признаков и усложняют алгоритм их обработки, применяют комбинированные извещатели, выбирают и устанавливают извещатели с учетом конкретной помеховой обстановки. Электрическая связь извещателей с приемно-контрольными приборами обеспечивается шлейфами. Приемно-контрольные приборы предназначены для одновременного приема сигналов тревоги от извещателей со световой и звуковой индикацией, передачи сигналов тревоги на пульт централизованного наблюдения, автоматического перехода на резервное автономное питание, формирования сигналов оповещения операторов в случае обрыва или короткого замыкания шлейфов. Для передачи извещений и команд управления на пульт централизованного наблюдения используются линии телефонной связи, специальные проводные линии, радиоканалы, комбинированные линии связи.

11. Основными средствами видеонаблюдения являются телевизионные камеры на ПЗС-матрицах и мониторы. Черно-белые телевизионные камеры повышенной четкости имеют разрешение 500–600 телевизионных линий (ТВЛ), цветные — 375–450 ТВЛ. Чувствительность типовых черно-белых камер составляет доли лк, цветных — единицы лк. Камеры высокой чувствительности обеспечивают наблюдение при лунном освещении (порядка 0,01 лк и менее). Для обеспечения приемлемого качества изображения в широком диапазоне освещенности объекта наблюдения, в том числе в мерцающем свете газоразрядных ламп, телевизионные камеры оснащаются электронным затвором, автоматическими диафрагмой и регулировкой усиления видеосигнала, устройствами гамма-коррекции, компенсации засветки и внешней синхронизации. По конструкции телевизионные камеры делятся на корпусные и бескорпусные. В зависимости от условий эксплуатации кожухи корпусных камер могут быть герметичными, с подогревом, с вентилятором, дворниками, омывателями стекол, иметь прочные («вандалоустойчивые») корпуса и окошки. Для осмотра пространства камеры могут устанавливаться на поворотных дистанционно управляемых платформах и оснащаться объективами с переменным фокусным расстоянием. В простейшем варианте видеосигнал с телевизионной камеры подается на монитор по проводному или радиоканалу.

Черно-белые и цветные мониторы имеют размеры экрана 7, 9, 12, 14, 15, 17 и 21 дюйм и разрешающую способность выше разрешающей способности телевизионных камер. Основной элемент мониторов — электронно-лучевая трубка (ЭЛТ), жидкокристаллическая или плазменная панель. Панели в силу существенных преимуществ постепенно вытесняют ЭЛТ. С целью снижения нагрузки на оператора при большом числе установленных камер и повышения эффективности видеоконтроля применяют видеокоммутаторы, видеоквадраторы, мультиплексоры, детекторы движения, специальные видеомагнитофоны и так называемые видеоменеджеры на базе компьютеров. Наиболее совершенные коммутаторы и квадраторы позволяют выводить на экран в любой последовательности и с временным интервалом изображения до 16 камер или одновременно формировать в нужном формате изображения от 4 и более камер, а также немедленно подключать к монитору камеру,

установленную в контролируемой зоне, из которой поступил сигнал тревоги. Современные видеомультиплексоры обладают широкими функциональными возможностями, в том числе позволяют просматривать на экране мониторов изображения от одних камер и записывать на видеомагнитофон сигналы от других камер. Записанные изображения могут просматриваться в полноэкранном формате, режимах квадрированного экрана, «картинки в картинке» и мультиэкрана. Мультиплексоры могут иметь встроенные детекторы движения, генераторы титров, даты и времени наблюдения. С детектором движения, который обнаруживает изменения в заданной области кадра изображения, у комплекса видеонаблюдения появляется возможность обеспечения автоматической видеоохраны. В специальных видеомагнитофонах за счет сжатия видеосигнала, уплотнения записи и пропуска кадров удается увеличить время записи на одной кассете до 40 суток. Кроме того, в этих видеомагнитофонах предусматривается дежурный режим с меньшим запаздыванием начала записи относительно момента подачи команды «Запись».

Для обеспечения наблюдения охраняемых зон в вечернее и ночное время создается дежурное освещение. В качестве источников света применяются вакуумные, криптоновые и галогенные лампы накаливания и газоразрядные лампы (газо- и паросветные, люминесцентные и электродосветные). Газоразрядные лампы имеют световую отдачу в 5–10 раз, а срок службы в 10–20 раз больше, чем лампы накаливания. Для скрытного телевизионного наблюдения применяются ИК-осветители — лампы накаливания, закрытые непрозрачными для видимого света фильтрами, и светодиоды.

12. Для задержания злоумышленника, проникшего в контролируемую зону, охрана может оснащаться резиновыми дубинками, газовым и огнестрельным оружием. В качестве звуковых охранных оповещателей применяются электромеханические звонки громкого боя, электромагнитные и пьезоэлектрические сирены с громкостью звука до 120 дБ. В качестве тревожной световой сигнализации могут использоваться источники яркого непрерывного или мигающего света в контролируемой зоне, включаемые автоматически по сигналу тревоги или вручную охраной. Для ликвидации пожара в любой организации в легкодоступных местах размещаются тради-

ционные средства пожаротушения: пенообразующие огнетушители, механические средства (багры, топоры) для разрушения очага пожара, бочки с песком, пожарные рукава и др. По способу пожаротушения установки пожаротушения делятся на объемные (локально-объемные) и поверхностные (локально-поверхностные). По степени автоматизации эти установки разделяют на автоматические, автоматизированные, ручные и роботизированные.

Автоматические установки водяного и пенного пожаротушения делятся на спринклерные (для локального тушения) и дренчерные (для тушения по площадям). Современные системы автоматического газового тушения заполняют газом помещение с очагом возгорания по сигналу «Пожар» от извещателей, установленных в этом помещении. Типовой комплекс содержит: модуль газового пожаротушения с баллонами газа, запорно-пусковым устройством, манометром и пиропатроном, размещаемыми в специальном помещении; пожарные (пожарно-охранные) извещатели и шлейфы; приемно-контрольный прибор, принимающий сигналы от извещателей и формирующий сигналы подрыва пиропатрона, отключения вентиляции, включения табло оповещения сотрудников о подаче газа; газопроводы от модуля к распылителям газа в помещениях; кнопки ручного пуска и его блокировки. Наряду с традиционными пенообразующими огнетушителями все шире применяются малогабаритные порошковые огнетушители. Тушение пожара с их помощью происходит как с участием человека, так и без него путем импульсного выброса огнетушащего порошка в зону возгорания.

При отключении основного электропитания 220 В 50 Гц включается автоматически или дежурным резервное или аварийное электропитание, обеспечивающее работоспособность средств охраны и видеонаблюдения, а также аварийного освещения. В качестве источников резервного электропитания применяются гальванические батареи, аккумуляторы и дизель-генераторы.

13. Подсистема защита информации от утечки не имеет столь четкой структуры, как подсистема физической защиты, но функционально ее можно разделить на комплексы защиты информации от наблюдения, подслушивания, перехвата и от предотвращения утечки информации по вещественному каналу.

Силы и средства защиты информации от наблюдения предназначены для: маскировки объектов наблюдения в видимом, инфра-

красном и радиодиапазонах электромагнитных волн; формирования и «внедрения» ложной информации об объектах наблюдения; уменьшения в случае необходимости прозрачности воздушной и водной сред; ослепления и засветки средств наблюдения в оптическом диапазоне; создания помех гидроакустическому и радиолокационному наблюдению.

Комплекс защиты информации от подслушивания включает средства, в основном, энергетического скрытия, предотвращающие утечку акустической информации в простом акустическом канале утечки информации. Эти средства должны обеспечить: звукоизоляцию и звукопоглощение речевой информации в помещениях; звукоизоляцию акустических сигналов работающих механизмов, по признакам которых можно выявить сведения, содержащие государственную или коммерческую тайну; акустическое зашумление помещения, в котором ведутся разговоры по закрытой тематике.

На средства защиты информации от перехвата возлагаются следующие задачи: структурное скрытие сигналов и содержащейся в них информации, подавление до допустимых значений уровней опасных сигналов в направляющих линиях связи (кабелях, волноводах), экранирование электрических, магнитных и электромагнитных полей с защищаемой информацией.

Средства предотвращения утечки информации по вещественному каналу должны обеспечить: уничтожение вещественных признаков в выбрасываемых или подлежащих дальнейшей переработке отходах; уничтожение неиспользуемых вещественных носителей; захоронение в специальных могильниках вещественных носителей, которые не могут быть уничтожены.

14. Эффективность системы защиты информации зависит от организации и работы сил и средств управления. Комплекс управления объединяет сотрудников и технические средства и выполняет следующие основные функции: прогноз возможных угроз защищаемой информации, планирование мер по обеспечению требуемого уровня безопасности информации и контроль их выполнения, контроль работоспособности средств защиты, сбор и анализ сигналов и данных об источниках угроз информации, формирование команд (сигналов) управления силам и средствами отражения и ликвидации угроз, анализ нарушений в функционировании системы и ее элементах, разработка мер по их предотвращению.

Комплекс управления включает центр (пункт) управления, руководителей и сотрудников организации, участвующие в управлении, а также средства управления подсистем, комплексов и подкомплексов. Источниками входных сигналов комплекса управления являются: вышестоящие органы управления и руководства организации, извещатели и приемно-контрольные приборы подкомплекса обнаружения источников угроз, телевизионные камеры и преобразователи видеосигналов, формирующие изображение для оператора, и сигналы тревоги, средства идентификации людей и автотранспорта, сотрудники службы безопасности, выявляющие технические каналы утечки информации и разрабатывающие меры по их ликвидации.

Для автоматизации процессов управления используются вычислительные ресурсы, базы данных и модели центра управления, сопрягаемые со средствами обнаружения, видеоконтроля, идентификации и нейтрализации угроз. Совокупность средств, объединяемых средствами управления, составляют техническую основу интегрированной системы охраны (ИСО).

В зависимости от состава средств интегрированные системы охраны различают по уровням. Система первого уровня (ИСО-1) объединяет средства охранной, пожарной и охранно-пожарной сигнализации и средства СКУД на территорию организации. ИСО-2 дополняется средствами видеонаблюдения. В ИСО-3 используется полный набор технических средств, в том числе СКУД в отдельные зоны, управление которыми осуществляется с помощью компьютеров. Интегрированные системы имеют иерархическую структуру и реализуются на базе адресных панелей, обслуживающих используемые датчики (охранные, охранно-пожарные, пожарные, считыватели электронных замков и др.) и исполнительные устройства (видеокамеры, оповещатели тревожной сигнализации, исполнительные механизмы замков, пиропатроны модулей газового пожаротушения и др.). Общее управление системой осуществляется одной или несколькими мощными ПЭВМ.

15. Основными средствами скрытия объектов наблюдения в оптическом диапазоне являются краски для маскировочного защитного, деформирующего и имитационного окрашивания, различные маски и экраны. Искусственные оптические маскировоч-

ные маски многоразового применения используются как маски-навесы, вертикальные маски, маски перекрытия, наклонные и радиопрозрачные маски. Для маскировки военной техники используются различные типы табельных маскировочных комплектов (МКТ). Комплект представляет собой металлический разборный каркас, на который натягивается окрашенная в различные цвета сплошная или сетчатая ткань. Светонепроницаемые одно- и многоцветные воздушные пены, быстро наносимые с помощью пеногенераторов на объекты, обеспечивают их эффективную маскировку в широком диапазоне длин волн в течение до нескольких часов. Дезинформирующее скрытие достигается с помощью деформирующих масок, ложных сооружений и конструкций. Для энергетического скрытия объектов наблюдения в помещении применяются шторы, занавески, жалюзи, тонированные стекла и пленки, на открытых пространствах — естественные и искусственные аэрозоли. Искусственные аэрозоли (дымовые завесы) для эффективного, но кратковременного скрытия объектов наблюдения создаются с помощью дымовых шашек, специальных боеприпасов, аэрозольных генераторов и дымовых машин. Для защиты объектов от наблюдения в ИК-диапазоне применяются различные теплоизолирующие экраны, в том числе подручные материалы с плохой теплопроводностью. Хорошими теплоизолирующими свойствами обладают воздушные пены. Для противодействия наблюдению с помощью оптических приборов применяются активные средства обнаружения оптики, представляющие собой приборы ночного видения с лазерной сканирующей подсветкой. Отраженный от стекла объектива оптического прибора луч лазера воспринимается на экране прибора ночного видения как точка повышенной яркости.

Структурное скрытие объектов радиолокационного наблюдения достигается с помощью средств, изменяющих распределение «блестящих точек» на радиолокационном изображении объекта. В качестве таких средств используются уголковые, линзовые, дипольные отражатели и переизлучающие антенные решетки. Для пассивного энергетического скрытия объектов от радиолокационного наблюдения его поверхность покрывают материалами, обеспечивающими градиентное и интерференционное поглощение облучающей электромагнитной энергии. Активное противодействие

радиолокационному наблюдению производится путем генерации помех.

Противодействие гидролокационному наблюдению обеспечивается путем: использования природных акустических экранов, покрытия поверхности объектов защиты материалами (нейлоном, полиэтиленом, полипропиленом, различными пластмассами, другими материалами, содержащими каучук), поглощающими акустические сигналы; создания активных помех гидролокаторам, в том числе путем ретрансляции облучающих сигналов с усилением их мощности.

16. К средствам пассивной защиты речевой информации в телефонных каналах, обеспечивающих структурное скрытие сигналов, относятся скремблеры и вокодеры. Информация в помещениях защищается с помощью средств звукоизоляции, глушителей и звукопоглощающих материалов. К средствам звукоизоляции относятся ограждения, экраны, кабины, кожухи и глушители. Ограждение — это стены, перекрытия, перегородки, окна и двери, имеющие по периметру контакты с другими ограждениями. Величина звукоизоляции ограждений зависит от многих факторов, в том числе пропорциональна частоте колебаний акустической волны, поверхностной массе ограждения, коэффициенту потерь материала ограждения и обратно пропорциональна собственной частоте колебаний ограждения, удельной плотности материала ограждения и скорости звука в материале ограждения. Для повышения звукоизоляции увеличивают количество слоев ограждений. В помещении наименьшую звукоизолирующую способность имеют двери и окна. Звукоизолирующая способность дверей повышается путем: устранения щелей между дверью и дверной коробкой с помощью уплотняющих прокладок из резины, порога или резинового фартука между дверью и полом; применением для дверного полотна более плотных пород дерева, увеличением толщины дверного полотна и обивки его дермантином или аналогичным материалом по слою войлока или ваты с валиком по периметру двери; установкой звукоизолирующей двери, выполненной в виде многослойного дверного полотна с размещением между слоями звукоизолирующего материала; установкой двойных дверей с тамбуром между ними шириной 20–30 см. Повышение звуко-

изоляции оконных проемов достигается: уплотнением притворов переплетов и стекол; применением уплотняющих прокладок и коробкой, обеспечивающих плотное закрытие окна; облицовкой периметра межстекольного пространства звукопоглощающим материалом; установкой оконных блоков с повышенной звукоизоляцией. Уплотнение частей окон повышает их звукоизоляцию приблизительно на 10 дБ, при облицовке межстекольного пространства по периметру звукопоглощающим покрытием она увеличивается еще примерно на 5 дБ. Акустические экраны используются для дополнительной защиты дверей, окон, технологических проемов, батарей отопления, панелей кондиционеров, отверстий воздушной вентиляции и других конструкций. Акустические экраны эффективны, если их размеры превышают в несколько раз длину волны звука. Для локальной звукоизоляции речевой информации применяют кабины 1–4 классов, изоляции акустических сигналов механизмов и машин — кожухи. Перспективными являются прозрачные переговорные кабины. Глушители в зависимости от способов глушения звука подразделяются на абсорбционные, реактивные и комбинированные. Поглощающая способность звукопоглощающих материалов обусловлена их пористой структурой, создающей большую поверхность, при взаимодействии с которой энергия акустической волны преобразуется в тепловую. По степени жесткости звукопоглощающие материалы делятся на мягкие, полужесткие и жесткие. Для повышения звукопоглощающей способности ограждений (стен, потолка, дверей) применяют пористые материалы с жестким каркасом (в виде плиток на пемзолите, оштукатуренных плит с заполнителем, плит из цементного фибролита), с полужестким каркасом в виде древесно-волокнистых и минераловатных плит и с упругим каркасом из полиуретанового пенопласта, пористого поливинихлорида, прошитых и обернутых в ткань маты из капронового волокна. Отдельную группу образуют мембранные и резонаторные звукопоглотители. Мембранные поглотители представляют собой тонкие плотные материалы, образующие мембраны, за которыми укрепляется демпирующий материал из поролона, губчатой резины, войлока и др. Резонаторные поглотители представляют собой перфорированные акустические экраны, поглощающие звук. Они применяются для экранирования нагревательных конструкций (отопительных батарей, панелей, стен).

17. Средства обнаружения, локализации и подавления закладных устройств объединяют средства радиоконтроля помещений, поиска неизлучающих закладных устройств и подавления закладных устройств. Средства радиоконтроля обнаруживают закладные устройства по излучаемым ими радиосигналам. Эти средства охватывают: обнаружители электромагнитных полей (индикаторы поля и частотометры), бытовые радиоприемники (без и с конвертами), специальные приемники (селективные микровольтметры, сканирующие радиоприемники, спектральные анализаторы, радиоприемники с встроенными излучателями акустических сигналов) и автоматизированные комплексы радиомониторинга. Типовой автоматизированный комплекс радиомониторинга состоит из сканирующего радиоприемника с набором антенн, компьютера типа Nootbook и программного обеспечения, позволяющего осуществлять в автоматизированном режиме поиск, обнаружение и локализацию радиоизлучающих закладных устройств. Комплекс может содержать контролер ввода информации, преобразователь спектра, а также генератор прицельной помехи для оперативного подавления сигналов закладного устройства в случае его обнаружения.

Поиск дистанционно управляемых закладных устройств или других средств, не излучающих во время поиска радиосигналы, производится по иным демаскирующим признакам: их полупроводниковым и металлическим элементам, непрозрачности корпусов и элементов для рентгеновских лучей, пустотам в местах установки таких закладных устройств. Наиболее эффективен поиск таких закладных устройств по их полупроводниковым элементам с помощью нелинейных локаторов. Различают нелинейные локаторы с непрерывным излучением и импульсные, с одним приемником, настроенным на 2-ю гармонику, и с двумя приемниками — для 2-й и 3-й гармоник. Частота излучения локаторов 680–1000 МГц. Мощность непрерывного излучения составляет не более 3–5 Вт, мощность в импульсе может достигать несколько сот Вт. За счет большей мощности импульсные локаторы имеют большую проникающую способность. Дальность обнаружения полупроводникового элемента 0,5–2 м, точность локализации — несколько см.

Металлодетекторы обнаруживают закладные устройства по электрическим и магнитным свойствам их токопроводящих эле-

ментов. По принципу действия различают параметрические (пассивные) и индукционные (активные) металлодетекторы, по конструкции — стационарные и ручные. В параметрических металлодетекторах токопроводящие элементы, попадающие в зону действия поисковой рамки диаметром 250–300 мм, изменяют ее индуктивность и частоту поискового генератора. Для измерения отклонения частоты используется метод «биений» колебаний поискового генератора и эталонного генератора стабильной частоты. Параметрические металлодетекторы по величине и знаку отклонения частоты позволяют разделять металлы по их магнитным свойствам: черные от цветных (парамагнитных и диамагнитных), но имеют невысокую чувствительность. Большей проникающей способностью и более высокой чувствительностью обладают индукционные (вихревые) металлодетекторы с 2 катушками. Поисковая катушка излучает переменное магнитное поле с частотой 3–20 кГц, а в измерительной катушке наводится ЭДС полем, переизлученным металлическими предметами. По виду сигнала, подаваемого в поисковую катушку, различают аналоговые и импульсные индукционные металлодетекторы. Максимальная чувствительность металлодетектора характеризуется обломком иглы длиной 5 мм, находящейся в поле действия измерительной катушки.

Для интероскопии предметов, в том числе стен, применяют переносные рентгеновские установки двух видов: флюороскопы и рентгенотелевизионные установки. В переносных флюороскопах теневое изображение просвечиваемого предмета наблюдается на люминесцентном экране просмотровой приставки, которое запоминается после выключения рентгеновской трубки. В рентгенотелевизионных установках теневое изображение преобразуется в телевизионное изображение на экране удаленного от излучателя монитора. Средства интерскопии позволяют наблюдать металлическую проволоку диаметром 0,15–0,2 мм и просвечивать бетонные стены толщиной до 100 см.

18. Средства предотвращения утечки информации через ПЭМИН должны подавлять опасные сигналы до значений, ниже чувствительности средств добывания — долей мкВ. Для подавления опасных сигналов случайных акустоэлектрических преобразователей используют: выключатели радиоэлектронных средств и

электрических приборов; фильтры низкой частоты с частотой среза в области нижней границы спектра речевого сигнала; цепочки полупроводниковых диодов, ослабляющих сигналы малых амплитуд; буферные устройства в виде эмиттерных повторителей, подавляющие опасные сигналы от их источника (например, громкоговорителя) и пропускающие полезные сигналы в прямом направлении практически без ослабления.

Для экранирования электромагнитных полей применяются специальные конструкции (экранные сооружения, помещения и камеры) и разнообразные материалы. Специальные конструкции выполняются из стальных листов толщиной 2–3 мм и обеспечивают ослабление электромагнитного поля на 60–120 дБ. Наиболее эффективными материалами для экранирования полей являются металлические листы и сетки. Стальные листы толщиной 2–3 мм, сваренные герметичным швом, обеспечивают наибольший экранирующий эффект (до 100 и более дБ). Однако коррозия и появляющиеся во время монтажа напряженность сварочных швов снижают надежность и долговечность экранов, а необходимые их периодической проверки и устранения дефектов повышают эксплуатационные расходы. Более дешевые и удобные, но менее эффективные экраны из металлической сетки, сплетенной из луженой стальной и латунной проволоки с ячейками размерами от долей до единиц мм. Все шире применяются фольговые и металлизированные материалы, токопроводящие краски и клеи, радиопоглощающие строительные материалы. В качестве фольговых материалов используются фольга толщиной 0,01–0,08 мм, наклеиваемая на экранируемую поверхность, и фольга на непроводящей подложке, например на фольгоизоле. Фольга изготовляется из алюминия, латуни, цинка. Из металлизированных материалов наиболее широко применяются металлизированные ткани и пленки (стекла). Ткани металлизируются путем вплетения в нее металлизированных или металлических нитей пряжи или нанесением на них распылением частиц металла струей сжатого воздуха. Их применяют для экранирования стен и оконных проемов (в виде штор), корпусов продукции, антенных отражателей, чехлов на объекты радиолокационного наблюдения. Стекла с токопроводящими покрытиями имеют поверхностное

электрическое сопротивление порядка 5–10 Ом при незначительном (не более 20%) ухудшении прозрачности. Токопроводящие пленки, наклеиваемые на стекла окон, позволяют повысить экранирующий эффект окон без ухудшения их внешнего вида и прозрачности на 18–22 дБ на частотах в сотни МГц и на 35–40 дБ на частотах единицы ГГц. Токопроводящие краски создаются путем ввода в краски токопроводящих материалов: коллоидного серебра, графита, сажи, оксидов металла, порошковой меди, алюминия и других металлов. Они в силу худшей электропроводности и малой толщины обеспечивают меньшую по сравнению с металлизированными тканями экранирующую эффективность, но не менее 30 дБ в широком диапазоне частот. Электропроводные клеи применяются вместо пайки и болтовых соединений элементов электромагнитных экранов, а также для заполнения щелей и малых отверстий в них. Путем добавки в бетон строительных конструкций удается также повысить экранирующие свойства стен и перекрытий зданий.

Для гарантированного ослабления опасных сигналов при жестких требованиях к уровню безопасности информации источники излучений размещают в экранированных помещениях (экранных комнатах), ограждения которых покрыты стальными листами или металлическими листами. Обычно экранные комнаты имеют площадь 6–8 м$^2$ при высоте 2,5–3 м. Металлические листы или полотнища сетки, покрывающие стены, потолок и пол, должны быть прочно, с малым электрическим сопротивлением, соединены между собой по периметру. Двери также экранируются с надежным электрическим контактом с экранами стен при их закрывании. При наличии в экранной комнате окон последние должны быть затянуты одним или двумя слоями сетки, расстояние между слоями двойной сетки — не менее 50 см. Экран, изготовленный из луженой низкоуглеродистой стальной сетки с размером 2,5–3 мм, уменьшает уровень излучений на 55–60 дБ, а из такой же двойной сетки с расстоянием между слоями 100 мм — на 90 дБ. При создании экранной комнаты необходимо одновременно обеспечить нормальные условия для работающего в ней человека, прежде всего, вентиляцию воздуха и освещение.

## Литература к разделу III


1. Техника получения изображений высокой четкости. Иностранная печать об экономическом, научно-техническом и военном потенциале государств — участников СЕГ и технических средствах его выявления. Серия: «Технические средства разведывательных служб зарубежных государств» // Ежемесячный информационный бюллетень ВИНИТИ. — 1996. — № 1. — С. 15–18.
2. *Варламов А. В., Кисиленко Г. А., Хорев А. А., Федоринов А. В.* Технические средства видовой разведки / Под ред. *А. А. Хорева*. — М.: РВСН, 1997, 327 с.
3. *Каторин Ю. Ф., Купренков Е. В., Лысов А. В., Остапенко А. Н.* Энциклопедия промышленного шпионажа. — СПб: Полигон, 2000, 512 с.
4. *Кириллов Д.* Ценная информация всегда в цене // Частный сыск, охрана, безопасность. — 1996. — № 7. — С. 26–30.
5. *Соловьева Н. М.* Фотокиноаппаратура и ее эксплуатация. — М.: Ленгпромбытиздат, 1992, 216 с.
6. Справочная книга радиолюбителя-конструктора. Книга 1. — М.: Радио и связь, 1993, 336 с.
7. *Юрьев С.* Сейфы и хранилища ценностей. Опыт сертификации на устойчивость к взлому // БДИ. — 1997. — № 2. — С. 99–101.
8. *Ш. Панканти, Рудд М. Болле, Энил Джейн.* Биометрия: будущее идентификации // Открытые системы. — 2000. — № 3 — С. 17–20.
9. *Макаров Г.* Пожарные извещатели // БДИ. — 2002. — № 2.
10. *Палий А. И.* Радиоэлектронная борьба. — М.: Воениздат, 1989, 350 с.
11. *Абалмазов Э. И.* Направленные микрофоны. Мифы и реальность // Системы безопасности связи и телекоммуникаций. — 1996. — № 4. — С. 90–100.

# Раздел IV. Организационные основы инженерно-технической защиты информации

## Глава 25. Организация инженерно-технической защиты информации

### 25.1. Задачи и структура государственной системы инженерно-технической защиты информации

Для обеспечения ИТЗИ необходимы силы и средства, техническая и нормативно-правовая база, а также постоянно проводимые мероприятия по ее обеспечению. Защиту информации обеспечивает ее владелец и пользователь. Защиту информации, содержащую государственную тайну, обеспечивают государственные органы и пользователи информации.

Инженерно-техническая защита информации проводится по двум основным направлениям: физическая защита носителя информации и ее скрытие. Предотвращением и нейтрализацией сил воздействия и утечки информации традиционно занимаются различные ведомства и органы, используются различные технические средства защиты информации.

Защита носителей информации в виде материальных тел не отличается от охраны любых других материальных ценностей. Охрану материальных ценностей от криминальных структур и элементов обеспечивают органы внутренних дел, а их защиту от пожара — соответствующие органы противопожарной безопасности Министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. Вопросами противодействия технической разведке эти органы не занимаются.

В разгар холодной войны, когда с, одной стороны, существенно возросли активность и технические возможности иностранных технических разведок, а с другой, — в условиях гонки вооружения стремительно увеличивался объем секретной информации, воз-

никла необходимость в создании специализированных органов по защите информации от технической разведки. Эти органы составляют основу государственной системы защиты информации, содержащей государственную тайну.

Структура **государственной системы защиты информации от технической разведки**, ее задачи и функции определены в Постановлении Совета Министров РФ от 15 сентября 1993 г. № 912-51 под названием «Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от утечки ее по техническим каналам».

Главными направлениями работ по защите информации являются:

- обеспечение эффективного управления системой защиты информации;
- определение состава сведений и демаскирующих признаков, охраняемых от технической разведки;
- анализ и оценка угроз безопасности информации;
- разработка организационно-технических мероприятий по защите информации и их реализация;
- организация и проведения контроля состояния защиты информации.

Основные задачи государственной системы защиты информации от технической разведки, сформулированные в этом положении, следующие:

- проведение единой технической политики, организация и координация работ по защите информации в различных сферах деятельности государства;
- исключение или существенное затруднение добывания информации техническими средствами разведки;
- принятие правовых актов, регулирующих отношения в области защиты информации;
- анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирования системы информационного обмена сведениями по осведомленности иностранных разведок;
- организация сил, создание средств защиты информации и контроля за ее эффективностью;

- контроль состояния защиты информации в органах государственной власти и на предприятиях.

Решение указанных задач осуществляется путем:

- предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;
- предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразователей;
- исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам. Несоответствия мер установленным требованиям или нормам по защите информации являются нарушениями, которые делятся на три категории:

- **первая** — невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;
- **вторая** — невыполнение требований или норм по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;
- **третья** — невыполнение других требований по защите информации.

Основными органами государственной системы защиты информации являются:

- Межведомственная комиссия по защите государственной тайны;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК) России;

- Федеральная служба безопасности (ФСБ) РФ;
- другие органы исполнительной федеральной власти и их структурные подразделения по защите информации;
- органы исполнительной власти субъектов федерации и их структурные подразделения;
- структурные подразделения и штатные специалисты по защите информации организаций (предприятий, учреждений).

Кроме того, косвенно в систему защиты информации входят органы МВД и МЧС, обеспечивающие физическую защиту материальных ценностей, в том числе источников информации.

Эти органы образуют три правовых уровня защиты информации: **федеральный, субъектов федерации и уровень предприятий (организаций)**. Так как количество органов по мере снижения уровня возрастает, то силы и средства государственной системы защиты информации образуют пирамиду. Наверху этой пирамиды находятся Межведомственная комиссия, Федеральная служба по техническому и экспортному контролю, ФСБ РФ, а основание образуют органы предприятий и организаций.

**Межведомственная комиссия по защите государственной тайны** образована Указом Президента РФ от 8 ноября 1995 г. № 1108. Положение о Межведомственной комиссии защите государственной тайны утверждено Указом Президента РФ № 71 от 20 января 1996 года. Межведомственная комиссия является коллегиальным органом, основная функция которого — координация деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ по защите государственной.

В соответствии с положением она имеет право:

- формировать перечень сведений, отнесенных к государственной тайне, и перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне; подготавливать и представлять в Правительство РФ предложения по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности;
- подготавливать для Правительства РФ предложения по организации разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих ре-

ализацию федерального законодательства о государственной тайне;

- рассматривать и представлять Президенту и Правительству РФ предложения по правовому регулированию вопросов защиты государственной тайны и совершенствованию системы защиты государственной тайны в РФ;
- определять порядок рассекречивания сведений, составляющих государственную тайну; организовывать работу межведомственных экспертных групп по рассекречиванию и продлению сроков засекречивания архивных документов; рассматривать запросы органов власти, предприятий, организаций, учреждений и граждан о рассекречивании сведений, отнесенных к государственной тайне;
- подготавливать для Правительства РФ экспертные заключения на документы, содержащие сведения, отнесенные к государственной тайне, в целях решения вопроса о возможности передачи указанных сведений другим государствам;
- подготавливать предложения по порядку определения размеров ущерба и рассматривать экспертные заключения о размерах ущерба, который может быть нанесен безопасности РФ вследствие несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого предприятиям, учреждениям, организациям и гражданам в связи с засекречиванием информации, находящейся в их собственности;
- давать заключения на решения органов государственной власти, которые могут привести к изменению перечня сведений, отнесенных к государственной тайне, приостанавливать или опротестовывать их решения;
- координировать работы по организации сертификации средств защиты, по лицензированию деятельности предприятий, учреждений и организаций, связанной с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Структуру Межведомственной комиссии образуют ее председатель, 2 заместителя, члены комиссии, ответственный секретарь, комиссии по рассекречиванию документов, межведомственные ра-

бочие и экспертные группы по направлениям деятельности, а также структурное подразделение центрального аппарата ФСТЭК России, осуществляющего организационно-техническое обеспечение деятельности Межведомственной комиссии.

**В Федеральную службу по техническому и экспортному контролю** РФ преобразована Указом Президента РФ от 9 марта 2004 г № 314 «О системе и структуре федеральных органов исполнительной власти» Государственная техническая комиссия при Президенте РФ. Государственная техническая комиссия СССР (Гостехкомиссия) впервые была создана для организации и координации работ по противодействию иностранной технической разведке Постановлением Совета Министров СССР от 18 декабря 1973 г. № 903-303. Ее образование вызвано научно-техническим прогрессом в 80-е годы в военной технике, прежде всего, широким внедрением в нее радиоэлектронных средств, создающих побочные электромагнитные излучения и наводки, а также наращиванием возможностей и активизацией деятельности иностранной технической разведки. Основной задачей Гостехкомисии СССР являлась в то время организация в стране комплексных работ по защите от иностранных технических разведок вооружения и военной техники, военных и военно-промышленных объектов [1].

В начале перестройки Гостехкомиссия СССР Указом Президента РФ от 5 января 1992 г. № 9 была преобразована в Государственную техническую комиссию при Президенте РФ, а в 2004 г. в ходе реорганизации структуры федеральных органов исполнительной власти преобразована, как уже указывалось выше, в Федеральную службу по техническому и экспортному контролю.

В соответствии с Указом Президента РФ от 16 августа 2004 г. № 1085 Федеральная служба по техническому и экспортному контролю является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечение безопасности информации в системах информационной в телекоммуникационной инфраструктуры, оказываю-

щих существенное влияние на безопасность государства в информационной сфере;
- противодействие иностранным техническим разведкам на территории Российской Федерации;
- обеспечение защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступам, предотвращения ее утечки ко техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля.

Так как Федеральная служба по техническому и экспортному контролю (в части функций Гостехкомиссии) является постоянно действующим федеральным органом исполнительной власти, деятельность которого направлена на защиту государственной и служебной тайны, то ее задачи в основном соответствуют задачам государственной системы защиты информации от технической разведки.

Федеральная служба по техническому и экспортному контролю РФ включает центральный аппарат, головную научную организацию по проблемам технической защиты (Государственный научно-исследовательский испытательный институт проблем технической защиты информации) и территориальные органы. Основными задачами этих органов являются [1]:

- проведение государственной политики по обеспечению эффективной защиты информации, содержащей государственную и служебную тайну, в органах государственной власти и местного самоуправления, на предприятиях, в учреждениях и организациях региона;
- организация методического обеспечения и координации деятельности по защите информации, составляющей коммерческую, банковскую и другие виды тайн в регионе.

При Гостехкомиссии (Федеральной службе по техническому и экспортному контролю) создана коллегия. Так как членами коллегии являются руководящие работники федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации, то решениями коллегии обеспечивается координация работ в области технической защиты информации в стране.

Деятельность **Федеральной службы безопасности РФ** (ФСБ) регламентируется Федеральным законом № 40-ФЗ от 3 апреля 1995 г. «Об органах Федеральной службы безопасности РФ» и «Положением о Федеральной службе безопасности РФ», утвержденной Указом Президента № 960 от 11 августа 2003 г. Для защиты государственной тайны на органы ФСБ возложены следующие основные функции:

- участие в разработке и реализации меры по защите сведений, составляющих государственную тайну, контроль за обеспечением сохранности этих сведений в федеральных органах государственной власти и органах государственной власти субъектов РФ, воинских формированиях и организациях;
- определение порядка осуществления контроля за обеспечением защиты сведений, составляющих государственную тайну, в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, воинских формированиях и организациях, а также порядка допуска граждан к сведениям, составляющим государственную тайну, приемом их на военную службу (работу) в органы и войска;
- определение порядка контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также за обеспечением защиты особо важных объектов (помещений) и находящихся в

них технических средств от утечки информации по техническим каналам;

- организация и осуществление шифровальной работы в органах ФСБ и войсках;
- организация и обеспечение эксплуатации, безопасности, развития и совершенствования открытой и засекреченной связи, систем оповещения и звукоусиления на объектах органов ФСБ и войск;
- регулирование в области разработки, производства, реализации, эксплуатации, ввоза в Российскую Федерацию и вывоза из Российской Федерации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, а также в области предоставления на территории Российской Федерации услуг по шифрованию информации и выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

организация и проведение исследований в области защиты информации, экспертных криптографических, инженерно-криптографических и специальные исследований шифровальных средств, специальных и закрытых информационно-телекоммуникационных систем;

подготовка экспертных заключений на предложения о проведении работ по созданию специальных и защищенных с использованием шифровальных (криптографических) средств информационно-телекоммуникационных систем и сетей связи;

- осуществление и организация лицензирования отдельных видов деятельности.

Структура ФСБ РФ, утвержденная Указом Президента РФ от 11 августа 2003 г. № 960, включает:

- центральный аппарат Федеральной службы безопасности РФ (департаменты, управления и другие подразделения, непосредственно реализующие направления деятельности органов федеральной службы безопасности, а также подразделения, исполняющие управленческие функции);
- территориальные органы безопасности (управления, отделы ФСБ по отдельным регионам и субъектам РФ);

- органы безопасности в войсках (управления, отделы в Вооруженных Силах, других войсках и воинских формированиях, а также в их органах управления);
- пограничные органы (управления, отряды, отделы ФСБ России по пограничной службе);
- другие органы.

Министерства, агентства, службы и другие органы решают в рамках своей компетенции следующие задачи по защите информации:

- конкретизируют перечень охраняемых сведений, составляющих государственную тайну;
- обеспечивают разработку и осуществление мер по защите информации в подведомственных организациях и предприятиях;
- организуют и координируют проведение научно-исследовательских и опытно-конструкторских работ в области защиты информации в соответствии с государственными (отраслевыми) программами;
- разрабатывают по согласованию с Гостехкомиссией отраслевые документы по защите информации;
- контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;
- создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;
- организуют подготовку и повышение квалификации специалистов по защите информации.

В министерствах, ведомствах, органах государственной власти субъектов Российской федерации организуются **Советы (Технические комиссии)** и **подразделения по защите информации**. Основными направлениями работы Советов являются:

- рассмотрение вопросов, связанных с защитой информации;
- координация и контроль выполнения работ по вопросам обеспечения защиты информации в отрасли (регионе);
- анализ и выработка рекомендаций по повышению эффективности защиты информации в отрасли (регионе).

На подразделения по защите информации возлагаются следующие основные функции:

- проведение единой технической политики, организация и координация работ по защите информации;

- организация аттестования подведомственных объектов по выполнению требований обеспечения защиты информации, сертификации средств защиты информации и контроля ее эффективности;
- организация и координация разработок, внедрение и эксплуатация систем мер по предотвращению утечки информации;
- организация и проведение работ по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;
- методическое обеспечение мер по защите информации;
- организация подготовки и повышения квалификации специалистов по вопросам защиты информации для подведомственных предприятий, учреждений и организаций, а также организация и проведение занятий с руководящим составом по вопросам защиты информации.

Работы по защите информации на предприятиях (в организациях и учреждениях) организуются их руководителями. Подразделения и штатные специалисты по безопасности на предприятиях осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне, определяют совместно с заказчиком работ основные направления комплексной защиты информации, участвуют в согласовании технических (тактико-технических) заданий на проведение работ, дают заключения о возможности проведения работ с информацией, отнесенной к государственной или служебной тайне.

В соответствии с существующим законодательством допуск предприятий (организаций, учреждений) к проведению работ, содержащих государственную тайну, созданию средств защиты информации и оказанию услуг по защите государственной тайны возможен после получении ими **лицензий** на соответствующий вид деятельности.

Органами, уполномоченными на ведение лицензионной деятельности, являются [6–8]:

- по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, — Федеральная служба безопасности РФ и ее территориаль-

ные органы (на территории РФ), Служба внешней разведки РФ (за рубежом);

- на право проведения работ, связанных с созданием средств защиты информации, — Федеральная служба по техническому и экспортному контролю РФ, Федеральная служба безопасности РФ, Служба внешней разведки РФ, Министерство обороны РФ (в пределах их компетенции);
- на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны — Федеральная служба безопасности РФ и ее территориальные органы, Федеральная служба по техническому и экспортному контролю РФ, Служба внешней разведки РФ (в пределах их компетенции).

В отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за деятельностью в области оказания услуг по защите информации.

Лицензии выдаются на срок 3–5 лет на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, и при выполнении следующих условий [6]:

- соблюдение требований законодательных и иных нормативных актов РФ по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения государственной тайны;
- наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

**Государственная аттестация руководителей предприятий** проводится методом собеседования с целью проверки их знаний, необходимых для организации на предприятии защиты сведений составляющих государственную тайну. Государственная аттеста-

ция руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами РФ, руководители которых наделены полномочиями по отношению к государственной тайне сведений в отношении подведомственных им предприятий.

**Специальная экспертиза предприятия** проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Специальные экспертизы организуются и проводятся [9]:

- Федеральной службой безопасности РФ и территориальными органами безопасности РФ, Федеральной службой по техническому и экспортному контролю РФ, другими министерствами и ведомствами РФ, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий;
- отраслевыми аттестационными центрами министерств и ведомств, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, для проведения специальных экспертиз на подведомственных им предприятиях;
- региональными аттестационными центрами Федеральной службы безопасности РФ и территориальными органами безопасности, Федеральной службы по техническому и экспортному контролю РФ, а также администрацией субъектов РФ, для проведения экспертиз на вневедомственных предприятиях.

Специальные экспертизы проводятся экспертными комиссиями при Федеральной службе безопасности РФ и территориальных органах безопасности, а также при аттестационных центрах.

**Контроль за соблюдением лицензионных условий** лицензиатами, выполняющими работы, связанные с использованием сведений, составляющие государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны осуществляют органы, уполномоченные на ведение лицензионной деятельности.

Технические средства, используемые для обработки защиты информации, должны иметь **сертификат соответствия** их характеристик требованиям по защите. Обязательной сертификации подлежат защищенные технические, программно-технические, программные средства, системы связи, сети и системы вычислительной техники, средства защиты и средства контроля эффективности защиты, а также технические и программные средства, предназначенные для обработки информации с ограниченным доступом, в том числе иностранного производства.

Сертификацию средств проводят Федеральная служба по техническому и экспортному контролю РФ, ФСБ РФ, Министерство обороны РФ, Служба внешней разведки РФ, аккредитованные органы по сертификации продукции, аккредитованные испытательные центры (лаборатории). Координация деятельности по сертификации возложена на Межведомственную комиссию по защите государственной тайны.

Объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, а также ведения секретных переговоров, подлежат обязательной аттестации на соответствие их требованиям стандартов или иных нормативно-технических документов, утвержденных Гостехкомиссией (Федеральной службой по техническому и экспортному контролю). Аттестационные испытания проводятся аттестационной комиссией, формируемой органом, аккредитованным Федеральной службой по техническому и экспортному контролю.

## 25.2. Организация инженерно-технической защиты информации на предприятиях (в организациях, учреждениях)

Предприятия (фирмы, организации, учреждения) — наиболее многочисленные структуры, в которых создается наибольший объем (количество) информации, содержащей государственную и конфиденциальную тайну. В них проводится конкретная и разнообразная работа по защите информации.

Независимо от формы собственности организация для проведения работ с информацией, содержащей государственную тайну, должна получить лицензию, т. е. выполнить предварительно в пол-

ном объеме требования по защите информации, предусмотренные соответствующими документами. После получения лицензии организация становится элементом государственной системы защиты информации, содержащей государственную тайну.

Для защиты информации, содержащей государственную тайну, на предприятии (в учреждении, организации) создаются в зависимости от объема работ по защите информации структурные подразделения или штатные специалисты, которые могут входить в состав одного из подразделений или службы безопасности. Их основными функции являются следующие:

- планирование работ по защите информации на предприятии (в учреждении, организации), разработка предложений по совершенствованию его системы защиты информации;
- определение демаскирующих признаков предприятия (учреждения, организации) и выпускаемой продукции;
- участие в подготовке предприятия (учреждения, организации) к аттестованию на право проведения работ с использованием сведений, отнесенных к государственной тайне;
- организация разработки нормативно-методических документов, разработка проектов распорядительных документов по вопросам организации защиты информации на предприятии;
- участие в согласовании ТЗ (ТТЗ) на проведение работ, содержащих государственную тайну, в разработке требований по защите информации при проведении исследований, разработке (модернизации), производстве и эксплуатации образцов продукции, при проектировании, строительстве и эксплуатации объектов (учреждения, организации);
- проведение периодического контроля эффективности мер защиты информации на предприятии (в учреждении, организации), участие в расследовании нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению нарушений;
- организация проведения занятий с руководящим составом и специалистами предприятия (учреждения, организации) по вопросам защиты информации.

Для защиты информации, составляющей коммерческую тайну, ее владелец создает собственную систему защиты информации.

Законодательно структура такой системы не закреплена. Она определяется многими факторами: видом деятельности, уровнем конфиденциальности информации и ее объемом, штатной численностью ее сотрудников, финансовым состоянием фирмы и др. Однако для любой фирмы однотипны объективные функции сил и средств обеспечения защиты информации. Их может выполнять как полноценная структура, включающее большое количество людей и технических средств, так и несколько человек для малой фирмы. В принципе, так же как в государственных структурах, каждый сотрудник фирмы должен в объеме должностных обязанностей обеспечивать защиту информации. Об этом он информируется при приеме на работу. Эти требования указываются, как правило, в договоре между работодателем и работником.

Наиболее полно вопросы организация системы безопасности фирмы рассмотрены в [2]. Система безопасности фирмы образует следующие основные элементы (должностные лица и органы):

- руководитель фирмы, курирующий вопросы безопасность информации;
- совет по безопасности фирмы;
- служба безопасности фирмы;
- подразделения фирмы, участвующие в обеспечении безопасности фирмы.

Руководство безопасностью возлагается, как правило, на руководителя фирмы и его заместителя по общим вопросам (1-го заместителя), которым непосредственно подчиняется служба безопасности.

Совет по безопасности фирмы представляет собой коллегиальный орган при руководителе фирмы, состав которого назначается им из числа квалифицированных и ответственных по вопросам информационной безопасности должностных лиц. Совет безопасности разрабатывает для руководителя предложения по основным вопросам обеспечения безопасности информации, в том числе: направлениям деятельности по обеспечению безопасности фирмы и ее подразделений, совершенствования системы безопасности, взаимодействия с органами власти, заказчиками, партнерами, конкурентами и потребителями продукции и др.

Структурные подразделения занимаются вопросами защиты информации, которую они создают или используют в своей де-

ятельности. Содержание и количество информации меняются во времени, в зависимости от решаемых задач и этапов деятельности. Однако основные и побочные результаты деятельности содержат защищаемую информацию еще длительное время, равное времени ее старения.

Служба безопасности является основным структурным подразделением по обеспечению безопасности, в том числе информационной, на фирме. Основными ее задачами в части информационной безопасности являются:

- мониторинг угроз информации;
- организация работы по защите информации на фирме;
- управление доступом сотрудником, автотранспорта и посетителей на территорию и в помещения фирмы;
- обеспечение безопасности информации при проведении всех видов деятельности внутри и вне фирмы, в том числе при чрезвычайных ситуациях;
- охрана территории, зданий, помещений и других мест и конструкций с защищаемой информацией.

Кроме этих задач служба безопасности обеспечивает охрану материальных ценностей фирмы и безопасность руководителей, ведущих специалистов и сотрудников.

Для решения указанных задач в полном объеме в службе безопасности создаются отдельные подразделения, примерный состав которых приведен на рис. 25.1.

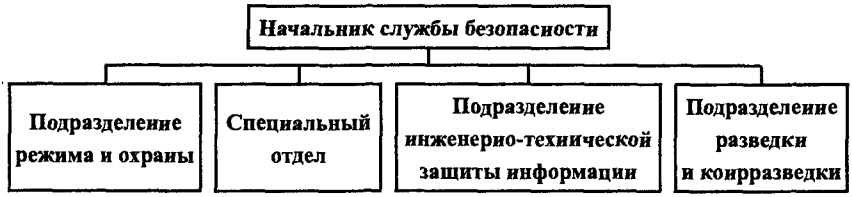



*Рис. 25.1.* Структура службы безопасности фирмы

**Подразделение режима и охраны** обеспечивает:

- организацию и контроль режима организации;
- охрану объектов организации и ее отдельных сотрудников, а также ценного груза при его перевозке за пределами организации.

В общем случае под режимом организации понимаются установленные законодательством, подзаконными актами и руководством организации условия работы в ней. В принципе для обеспечения эффективной деятельности любой организация в ней устанавливается определенный режим работы сотрудников. Если технологический процесс производства продукции непрерывен, то этот процесс должны обеспечивать сотрудники независимо от выходных, праздников, болезни и других обстоятельств. Например, нельзя временно, на праздники, потушить доменную печь, так как после этого нельзя восстановить ее работу без почти катастрофических последствий.

Однако обычно режим предполагает условия работы, направленные на обеспечение безопасности ценностей, в том числе информации. В этом смысле организацию с таким режимом называют **режимной**.

Ответственные сотрудники подразделения режима и охраны не только конкретизируют документы вышестоящих организация по режиму и разрабатывают внутри объектовые документы, но и контролируют выполнение их работниками организации. Например, сотрудники подразделения осматривают подозрительные предметы, которые могут вносить (ввозить) или выносить (вывозить) работники и посетители, контролируют способы переноса и хранения продукции с защищаемыми признаками, надежность закрытия и состояние печатей запасных дверей и ворот, порядок сдачи выделенных помещений под охрану и их вскрытия и др. Сотрудники подразделения режима и охраны занимаются также расследованием нарушений режима в организации.

Основу санкционированного доступа в контролируемые зоны составляет **пропускной режим**. Традиционно пропускной режим обеспечивается с помощью удостоверений и пропусков. Пропуска для сотрудников и посетителей могут быть постоянными, временными и разовыми, а также материальные для ввоза и вывоза материальных ценностей. Постоянные документы выдаются на несколько лет с последующей перерегистрацией или заменой, временные на несколько месяцев, разовые — на один день. Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством организации. Однако эти доку-

менты относятся к атрибутным идентификаторам со всеми присущими им недостатками. Их постепенно вытесняют более защищенные атрибутные идентификаторы (карты на различных принципах работы) и биометрические идентификаторы.

Для охраны объектов организации привлекаются в зависимости от их ведомственной принадлежности силы и средства подразделений охраны МО, МВД и коммерческих охранных структур, а также создаются собственные группы охраны. При использовании внешних сил охраны подразделение режима осуществляет контроль за выполнением ими своих функций. Группа охраны организации входит в состав ее подразделения режима и охраны и осуществляет охрану и контроль собственными силами.

**Специальный отдел** обеспечивает учет всех грифованных документов (входящей и исходящей корреспонденции, разрабатываемых и размножаемых в организации документов), циркулирующих в организации, ее централизованное хранение и санкционированной доступ к ней сотрудников организации. В специальном отделе учитывают также образцы продукции (веществ, макетов, узлов и др.), содержащие защищаемую информацию. Основанием для выдачи сотрудников документов и образцов продукции служат временные и разовые допуски, оформляемые руководителями структурных подразделений.

Защита информации с помощью инженерных конструкций и технических средств возлагается на **подразделение инженерно-технической защиты информации**. Оно занимается выявлением потенциальных угроз, разработкой мер по их предотвращению, инструментальным контролем уровней опасных сигналов и эксплуатацией технических средств защиты информации.

Любая организация, в том числе принадлежащая государству, нуждается для обеспечения эффективной деятельности в информации о партнерах и конкурентах. Для добывания этой информации в рамках как деловой разведки, так и промышленного шпионажа создается в организации **подразделение разведки** и **контрразведки**. Это подразделение обеспечивает:

- добывание данных и сведений и их аналитическую обработку с целью получения разведывательной информации о партнерах и конкурентах;

- прогнозирование угроз информации организации со стороны конкурентов и иных злоумышленников;
- разработка предложений по контрразведывательному обеспечению информационной безопасности.

Основная часть информации (по некоторым оценкам, до 95%) добывается из открытых источников, в особенности по вопросам, касающимся тенденций рынка, потенциальных конкурентов, надежности фирм, с которыми собирается сотрудничать организация и др. Однако информация об оригинальных схемотехнических, конструкторских и технологических решениях, реализация которых в продукции может обеспечить ее владельцам существенные преимущества перед конкурентами, закрывается и защищается.

## 25.3. Нормативно-правовая база инженерно-технической защиты информации

Деятельность государственной системы защиты информации регламентируется документами, составляющими нормативно-правовую базу инженерно-технической защиты информации. Основу ее составляют документы, классификация которых приведена на рис. 25.2.

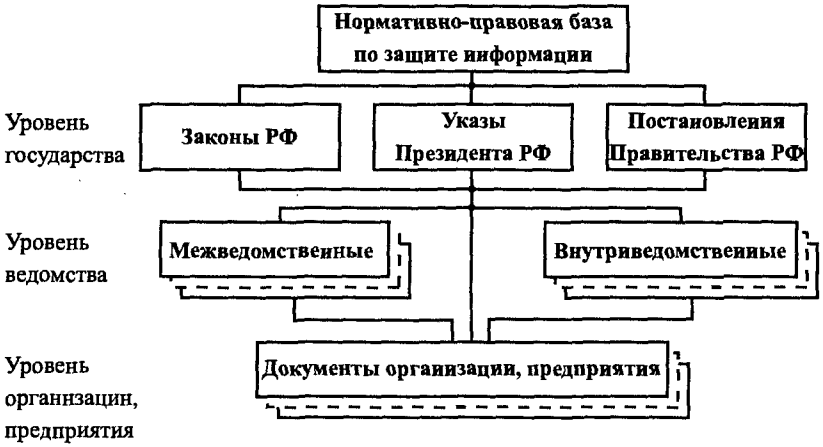



*Рис. 25.2.* Классификация документов нормативно-правовой базы по защите информации

По назначению документы делятся на:

- руководящие;
- нормативные;
- методические.

**Руководящие документы** определяют структуру, права и обязанности органов и людей, обеспечивающих инженерно-техническую защиту информации на различных уровнях государственной системы. Руководящие документы разрабатываются на всех уровнях государственной системы защиты информации, причем документы на более низком уровне конкретизируют документы более высокого уровня.

Любая деятельность по выполнению руководящих документов сопровождается принятием решений по тому или иному вопросу. Основу принятия решений составляет идентификация текущих факторов или признаков с эталонными. Совокупность эталонных факторов или признаков представляют собой сущность понятия «норма» и содержание нормативных документов. Понятие нормы широко используется во всех сферах деятельности людей. Например, в обществе существуют нормы поведения, часть которых законодательно закреплена в Гражданском кодексе. Грубые отклонения от норм поведения — преступления и шкала наказаний в зависимости от уровня отклонения от нормы рассмотрены в Уголовном кодексе. Нормы в человеческом обществе могут изменяться эволюционно в процессе его развития и трансформироваться отдельными группами людей, обладающих силами и средствами психологического воздействия на население.

**Нормативы** в области инженерно-технической защиты информации определены специалистами в нормативных документах. В результате сравнения текущих показателей защиты информации с требуемыми нормативами принимается решение об уровне безопасности защищаемой информации.

Так как текущие показатели эффективности защиты информации зависят от большого числа факторов, то **методики** их определения разными органами и специалистами и, следовательно, полученные результаты в общем случае могут отличаться. Например, если не совпадают методики измерения уровней опасных сигналов у контролирующего и контролируемого органов, то специалистам

контролируемого органа трудно доказать достаточность использованных мер защиты. Поэтому, как правило, одновременно разрабатываются нормативы и **методики** их определения, которые объединяются в нормативно-методические документы.

Основные законы РФ, указы Президента РФ и Постановления Правительства РФ в области инженерно-технической защиты информации указаны в табл. 25.1.

*Таблица 25.1*

| *№ п/п* | *Уровень документа* | *Наименование документа* | *Дата принятия* | *№ документа* |
|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* |
| 1 | Законы РФ | О государственной тайне | 21 июня 1993 г. | 5485-1 |
| | | Об информации, информатизации и защите информации | 20 февраля 1995 г. | 24-ФЗ |
| | | О безопасности | 5 марта 1992 г. | 2446-1 |
| | | О федеральных органах правительственной связи и информации | 19 февраля 1993 г. | 4524-1 |
| | | О связи | 16 февраля 1995 г. | 15-ФЗ |
| | | Об органах Федеральной службы безопасности в Российской Федерации | 22 февраля 1995 г. | 40-ФЗ |
| | | Об участии в международном информационном обмене | 4 июля 1996 г. | 85-ФЗ |
| 2 | Указы Президента РФ | Положение о Федеральной службе по техническому и экспортному контролю | 6 августа 2004 г. | 1085 |
| | | Вопросы защиты государственной тайны | 30 марта 1994 г. | 614 |
| | | Об утверждении перечня сведений, отнесенных к государственной тайне | 8 ноября 1995 г. | 1108 |
| | | Об утверждении перечня сведений конфиденциального характера | 6 марта 1997 г. | 644 |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| | | О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам | 8 мая 1993 г. | 188 |
| 3 | Постановления правительства РФ | Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности | 4 сентября 1995 г. | 870 |
| | | О лицензировании отдельных видов деятельности | 24 декабря 1994 г. | 1418 |
| | | О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий (или) оказанием услуг по защите государственной тайны | 15 апреля 1995 г. | 333 |
| | | Положение о сертификации средств защиты информации | 26 июня 1995 г. | 608 |
| | | Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти | 3 ноября 1994 г. | 1233 |
| | | О лицензировании деятельности по технической защите конфиденциальной информации | 30 апреля 2002 г. | 135 |

Основу межведомственных документов составляют решения, руководящие и нормативно-методические документы ФСТЭК (Гостехкомиссии). В них рассматриваются основы концепции защиты информации от технической разведки, типовые положения об органах по защите информации, требования и методические рекомендации по защите информации от утечки по техническим кана-

лам, руководящие документы по различным аспектам защиты информации в автоматизированных системах, нормативно-методические документы по противодействию различным видам технической разведки.

В каждом ведомстве государства, являющемся владельцем или пользователем информации, содержащим государственную тайну, разрабатываются и конкретизируются руководящие и нормативно-методические документы и создаются органы, обеспечивающие защиту информации как в самом ведомстве, так и подчиненных подразделениях (организациях, предприятиях).

К руководящим документам, разрабатываемым в организации (на предприятии), относятся:

- руководство (инструкция) по защите информации в организации (на предприятии);
- положение о подразделении организации, на которое возлагаются задачи по обеспечению безопасности информации;
- инструкции по защите отдельных источников информации, прежде всего информации о разрабатываемых изделиях и продукции.

В различных организациях эти документы могут иметь разные наименования, отличающиеся от указанных. Но сущность этих документов остается неизменной, так как необходимость в них объективна.

Порядок защиты информации в организации определяется соответствующим руководством (инструкцией). Оно может содержать следующие разделы:

- общие положения;
- перечень охраняемых сведений;
- демаскирующие признаки объектов организации;
- оценки возможностей органов и средств добывания информации;
- организационные и технические мероприятия по защите информации;
- порядок планирования работ службы безопасности;
- порядок взаимодействия с государственными органами, решающими задачи по защите материальной и интеллектуальной собственности, государственной и коммерческой тайны.

Но в данном руководстве нельзя учесть всех особенностей защиты информации в конкретных условиях. В любой организации постоянно меняется ситуация с источниками и носителями конфиденциальной информации, угрозами ее безопасности. Например, появлению нового товара на рынке предшествует большая работа, включающая различные этапы и стадии: проведение исследований, разработка лабораторных и действующих макетов, создание опытного образца и его доработка по результатам испытаний, подготовка производства (документации и дополнительного оборудования), изготовление опытной серии для выявления спроса на товар, массовый выпуск продукции.

На каждом этапе и стадии к работе подключаются новые люди, разрабатываются новые документы, создаются узлы и блоки с информативными для них демаскирующими признаками. Созданию каждого изделия или самостоятельного документа сопутствует свой набор информационных элементов, их источников и носителей, угроз и каналов утечки информации, проявляющихся в различные моменты времени.

Для защиты информации об изделии на каждом этапе его создания разрабатывается соответствующая инструкция. Инструкция должна содержать сведения, необходимые для обеспечения безопасности информации, в том числе: общие сведения об образце, защищаемые сведения о нем и его демаскирующие признаки, потенциальные угрозы безопасности информации, замысел и меры по защите, порядок контроля (задачи, органы контроля, имеющие право на проверку, средства контроля, допустимые значения контролируемых параметров, условия и методики, периодичность и виды контроля), фамилии лиц, ответственных за безопасность информации.

Нормативно-методическую базу составляют [3]:

- государственные стандарты (ГОСТы);
- общие требования (ОТ), общие технические требования (ОТТ), тактико-технические требования (ТТТ), руководящие документы (РД) и другие документы;
- модели;
- нормы, методики и инструкции;

- эксплуатационно-техническая документация;
- учебно-методическая и научная литература.

Перечень основных государственных стандартов на технические средства охраны указан в табл. 25.2.

*Таблица 25.2*

| *№ п/п* | *Номер ГОСТа* | *Наименование ГОСТа* |
|---|---|---|
| *1* | *2* | *3* |
| 1 | ГОСТ 26342-84 | Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры |
| 2 | ГОСТ 4.188-85 | Средства охранной, пожарной и охранно-пожарной сигнализации. Номенклатура показателей |
| 3 | ГОСТ 27990-88 | Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования |
| 4 | ГОСТ Р 50009-92 | Совместимость технических средств охранной, пожарной и охранно-пожарной сигнализации электромагнитная. Требования, нормы и методы испытаний на помехоустойчивость и индустриальные радиопомехи |
| 5 | ГОСТ Р 50658-94 | Системы тревожной сигнализации. Часть 2. Требования к системам охраной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений |
| 6 | ГОСТ Р 50659-94 | Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Часть 5. Радиоволновые доплеровские извещатели для закрытых помещений |
| 7 | ГОСТ Р 50775-95 (МЭК 839-1-88) | Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения |
| 8 | ГОСТ Р 50776-05 (МЭК 839-14-89) | Системы тревожной сигнализации. Часть 1. Системы охранной сигнализации. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию |
| 9 | ГОСТ Р 50777-95 (МЭК 839-1-6-90) | Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для помещений |

| 1 | 2 | 3 |
|---|---|---|
| 10 | ГОСТ Р 50862-96 | Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость |
| 11 | ГОСТ Р 50941-96 | Кабины защитные. Общие технические требования и испытания |
| 12 | ГОСТ Р 51072-97 | Двери защитные. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому |
| 13 | ГОСТ Р-51053 | Замки сейфовые. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому |
| 14 | ГОСТ Р 5089-97 | Замки и защелки для дверей. Технические условия |
| 15 | ГОСТ 51136-98 | Стекла защитные многослойные. Общие технические условия |
| 16 | ГОСТ Р 51186-98 | Системы тревожной сигнализации. Требования и методы испытаний систем охранной сигнализации. Извещатели акустические пассивные для блокирования остекленных конструкций в закрытых помещениях |
| 17 | ГОСТ Р 51241-98 | Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытаний |
| 18 | ГОСТ Р 51558-2000 | Системы охранные телевизионные. Общие технические требования и методы испытаний |

Основным нормативным документом является перечень сведений, составляющих государственную, военную, коммерческую или любую другую тайну. Перечень сведений, содержащих государственную тайну, основывается на положениях Закона «О государственной тайне»». Перечни подлежащих защите сведений этого закона конкретизируются ведомствами применительно к тематике конкретных организаций. В коммерческих структурах, выполняющих государственные заказы, перечни распространяются на информацию, относящуюся к этому заказу. Перечни сведений, составляющих коммерческую тайну, составляются руководством фирмы при участии сотрудников службы безопасности.

Другие нормативные документы определяют максимально допустимые значения уровней сигналов с защищаемой информацией

и концентрации демаскирующих веществ на границах контролируемых зон, непревышение которых обеспечивает требуемый уровень безопасности информации. Эти нормы разрабатываются соответствующими ведомствами, а для коммерческих структур, выполняющих негосударственные заказы, — специалистами этих структур. Кроме того, нормативные документы объединены с методиками измерения параметров норм.

Работа по защите информации в организации проводится всеми его сотрудниками, но степень участия различных категорий существенно отличается. Любой сотрудник, подписавший обязательство о неразглашении тайны, участвует в защите информации хотя бы путем выполнения руководящих документов о защите информации.

### Вопросы для самопроверки

1. Основные задачи государственной системы защиты информации от технической разведки.
2. Сущность категорий нарушений требований по защите информации.
3. Структура государственной защиты информации от технической разведки.
4. Задачи и структура Федеральной службы по техническому и экспортному контролю РФ (Государственной технической комиссии).
5. Задачи и структура органов по защите информации Федеральной службы безопасности России.
6. Задачи органов по обеспечению защиты информации ведомств.
7. Виды и органы лицензирования продукции, деятельности и услуг по защите информации.
8. Задачи и органы, обеспечивающие сертификацию средств по защите информации.
9. Задачи и структура по защите информации в организациях (учреждениях, на предприятиях).
10. Классификация документов нормативно-правовой базы по защите информации.
11. Назначение руководящих и нормативно-методических документов по защите информации.

# Глава 26. Типовые меры по инженерно-технической защите информации

## 26.1. Основные организационные и технические меры по обеспечению инженерно-технической защиты информации

На предприятиях (в организациях, учреждениях) работа по инженерно-технической защите информации включает два этапа:

- построение или модернизация системы защиты;
- поддержание защиты информации на требуемом уровне.

Построение системы защиты информации проводится во вновь создаваемых организациях, в остальных — модернизация существующей. Методические вопросы построения и модернизации системы защиты информации рассмотрены в разделе V.

Построение (модернизация) системы защиты информации и поддержание на требуемом уровне ее защиты в организации предусматривают проведение следующих основных работ:

- уточнение перечня защищаемых сведений в организации, определение источников и носителей информации, выявление и оценка угроз ее безопасности;
- определение мер по защите информации, вызванных изменениями целей и задач защиты, перечня защищаемых сведений, угроз безопасности информации;
- контроль эффективности мер по инженерно-технической защите информации в организации.

Меры по защите информации целесообразно разделить на две группы: организационные и технические. В публикациях, в том числе в некоторых руководящих документах, меры по защите делят на организационные, организационно-технические и технические. Учитывая отсутствие достаточно четкой границы между организационно-техническими и организационными, организационно-техническими и техническими мерами, целесообразно ограничиться двумя группами: организационными и техническими. Но даже при такой дихотомической классификации граница между организационными и техническими мерами размыта. Например, при уп-

равлении доступом все шире применяются технические средства аутентификации.

Классификация **организационных мер** ИТЗИ приведена на рис. 26.1.

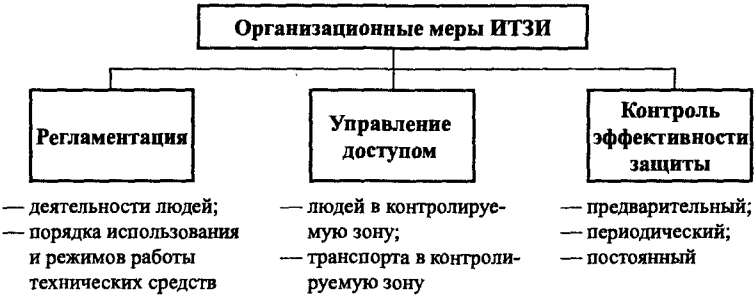



*Рис. 26.1.* Структура организационных мер

Организационные меры инженерно-технической защиты информации являются частью ее организационной защиты, основу которой составляют регламентация и управление доступом. Организационные меры инженерно-технической защиты информации определяют порядок и режимы работы технических средств защиты информации.

**Регламентация** — это установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленных на обеспечение безопасности информации.

Регламентация предусматривает:

- установление границ контролируемых и охраняемых зон;
- определение уровней защиты информации в зонах;
- регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т. д.);
- определение режимов работы технических средств, в том числе сбора, обработки и хранения защищаемой информации на ПЭВМ, передачи документов, порядка складирования продукции и т. д.

Например, в распорядке дня работы организации для исключения копирования секретных документов ее сотрудниками определяются правила работы с секретными документами после окончания рабочего дня. Другой пример — установление времени работы с секретными документами в электронном виде на компьютере, в течение которого для исключения утечки информации через ПЭМИН включаются генераторы радиопомех.

**Управление доступом** к информации включает мероприятия, обеспечивающие санкционированный доступ к ней людей, средств и сигналов. Оно предусматривает:

- идентификацию лиц и обращений;
- проверку полномочий лиц и обращений;
- регистрацию обращений к защищаемой информации;
- реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений по каналам телекоммуникаций проводится с целью их надежного опознавания.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

Реагирование на любое обращение к информации заключается либо в разрешении доступа к информации, либо в отказе. Отказ может сопровождаться включением сигнализации, оповещением службы безопасности или правоохранительных органов, задержанием злоумышленника при его попытке несанкционированного доступа к защищаемой информации.

К **техническим** относятся меры, реализуемые путем установки новых или модернизации используемых инженерных конструкций и технических средств защиты информации. Технические меры предусматривают применение методов, способов и средств, типовой перечень которых приведен в табл. 26.1.

*Таблица 26.1*

| *№ п/п* | *Вид угрозы* | *Методы защиты* | *Средства инженерно-технической защиты* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1 | Преднамеренные воздействия злоумышленников на источники информации | Укрепление механической прочности рубежей | Инженерные конструкции: бетонные заборы, колючая проволока, толстые стены и перекрытия, решетки и пленки на окнах, металлические двери, хранилища и сейфы |
| | | Обнаружение злоумышленников | Охранные извещатели, телевизионные средства наблюдения |
| | | Нейтрализация преднамеренных воздействий | Средства тревожной сигнализации, оружие, средства пожаротушения, средства резервного электропитания |
| 2 | Пожар | Уменьшение теплопроводности среды | Огнеупорные сейфы помещения |
| | | Обнаружение пожара | Пожарные извещатели |
| | | Нейтрализация пожара | Огнетушители, автоматические системы пожаротушения |
| 3 | Наблюдение | Пространственное скрытие объектов наблюдения | Тайники |
| | | Временное скрытие объектов наблюдения | Чехлы, естественные и искусственные маски во время работы средств наблюдения |
| | | Маскировка объектов наблюдения | Естественные и искусственные маски, краски для маскировочного окрашивания, ложные объекты, пеиы, дымы, уголковые отражатели, линзы Люнеберга, средства уменьшения ЭПР объекта радиолокационного наблюдения (маски, поглощающие материалы) |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | Засветка и ослепление | Яркие источники света, дипольные отражатели, генераторы помех радиолокационным станциям |
| 4 | Подслушивание | Кодирование слов речевого сообщения. Кодирование символов сообщения | Шифраторы |
| | | Частотно-временное преобразование сигналов | Скремблеры |
| | | Цифровое шифрование медленно изменяющихся характеристик речевых сигналов | Вокодеры |
| | | Звукоизоляция и звукопоглощение | Ограждения, акустические экраны, кабины, кожухи, глушители, звукопоглощающие материалы |
| | | Снижение уровня опасных электрических и радиосигналов | Средства отключения радиоэлектронных средств, фильтры опасных сигналов, ограничители малых амплитуд, буферы, экраны, конденсаторы для симметрирования кабелей, генераторы линейного и пространственного зашумления |
| | | Обнаружение, локализация и изъятие закладных устройств | Обнаружители поля, интерсепторы, бытовые радиоприемники с конверторами,специальныерадиоприемники, анализаторы спектра, сканирующие радиоприемники, автоматизированные комплексы радиомониторинга, металлодетек- |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | | торы, нелинейные локаторы, обнаружители пустот, средства интерскопии, средства контроля напряжения и тока телефонных линий, измерители электрических параметров телефонных линий, кабельные радары, средства обнаружения скрытно работающих диктофонов, средства нарушения работы и уничтожения закладных устройств, генераторы прицельной и заградительной помехи |
| 5 | Перехват | | Экраны, средства передачи информации широкополосными сигналами и сигналами с псевдослучайным изменением частоты, генераторы помех |
| 6 | Сбор и анализ отходов производства | | Шредеры, устройства магнитного стирания, механические прессы, средства очистки демаскирующих веществ |

Меры, определяющие порядок использования этих средств, составляют основу организационных мер инженерно-технической защиты информации.

## 26.2. Контроль эффективности инженерно-технической защиты информации

Важнейшее и необходимое направление работ по защите информации — **контроль эффективности защиты информации**. Контроль проводится силами службы безопасности, руководителями организации и структурных подразделений, всеми сотрудниками организации, допущенными к закрытой информации.

Применяют следующие виды контроля:

- предварительный;
- периодический;
- постоянный.

**Предварительный контроль** проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в том числе:

- после установки нового технического средства защиты или изменения организационных мер;
- после проведения профилактических и ремонтных работ средств защиты;
- после устранения выявленных нарушений в системе защиты.

**Периодический контроль** осуществляется с целью обеспечения систематического наблюдения за уровнем защиты. Он проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всей организации) по планам, утвержденным руководителем организации, а также вышестоящими органами.

Наиболее часто должен проводиться периодический контроль на химических предприятиях, так как незначительные нарушения в технологическом процессе могут привести к утечке демаскирующих веществ. Для определения концентрации демаскирующих веществ регулярно берутся возле предприятия пробы воздуха, воды, почвы, снега, растительности.

Периодичность и места взятия проб определяются характером производства с учетом условий возможного распространения демаскирующих веществ, например розы ветров и скорости воздушных потоков, видов водоемов (искусственный, озеро, болото, река и др.), характера окружающей местности и т. д. Пробы воздуха рекомендуется брать с учетом направлений ветра на высоте примерно 1,5 м в непосредственной близости от границ территории (50–100 м) и в зоне максимальной концентрации демаскирующих веществ, выбрасываемых в атмосферу через трубы. Пробы воды берутся в местах слива в водоемы в поверхностном слое и на глубине 30–50 см с последующим смешиванием. Берутся также пробы почвы и пыли на растительности. С этой целью собирают листья с нескольких деревьев и кустов на уровне 1,5–2 м от поверхности и не ранее недели после дождя.

Периодический (ежедневный, еженедельный, ежемесячный) контроль должен проводиться также сотрудниками организации в части источников информации, с которыми они работают.

Общий (в рамках всей организации) периодический контроль проводится временными внутренними и внешними комиссиями обычно 2 раза в год. Целью его является тщательная проверка работоспособности всех элементов и системы защиты информации в целом. Так как о времени работы комиссии сотрудникам организации (предприятия) заранее известно, то эти проверки выявляет в основном недостатки, не устраненные перед началом работы комиссии.

**Постоянный контроль** осуществляется выборочно силами службы безопасности и привлекаемых сотрудников организации с целью объективной оценки уровня защиты информации и, прежде всего, выявления слабых мест в системе защиты организации. Так как объекты и время такого контроля сотрудникам не известны, то такой контроль, кроме того, оказывает психологическое воздействие на сотрудников организации, вынуждая их более тщательно и постоянно выполнять требования по обеспечению защиты информации.

Следует также отметить, что добросовестное и постоянное выполнение сотрудниками организации требований по защите информации основывается на рациональном сочетании способов принуждения и побуждения.

**Принуждение** — способ, при котором сотрудники организации вынуждены соблюдать правила обращения с источниками и носителями конфиденциальной информации под угрозой административной или уголовной ответственности.

**Побуждение** предусматривает создание у сотрудников установки на осознанное выполнение требований по защите информации, формирование моральных, этических, психологических и других нравственных мотивов. Воспитание побудительных мотивов у сотрудников организации является одной из задач службы безопасности, но ее усилия найдут благодатную почву у тех сотрудников, которые доброжелательно относятся к руководству организации и рассматривают организацию как долговременное место работы. Создание условий и традиций, при которых место работы воспринимается как второй дом, является, по мнению компетентных аналитиков, одним из факторов экономического роста Японии. Поэтому на строгость и точность выполнения сотрудни-

ками требований по защите информации в значительной степени влияет климат в организации, который формируется ее руководством.

Эффективность защиты информации от технической разведки оценивается методами **технического контроля**. В ходе его производится определение технических параметров носителей информации. В результате сравнения их с нормативными значениями принимается решение об уровне безопасности защищаемой информации.

Технические меры контроля проводятся с использованием технических средств радио- и электрических измерений, физического и химического анализа и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемых зон;
- уровней опасных сигналов и помех в проводах и экранах кабелей, выходящих за пределы контролируемой зоны;
- степени зашумления генераторами помех структурных звуков в ограждениях;
- концентрации демаскирующих веществ в отходах производства.

Для измерения напряженности электрических полей используются селективные вольтметры, анализаторы спектра, панорамные приемники.

Различают три вида технического контроля:

- инструментальный;
- инструментально-расчетный;
- расчетный.

**Инструментальные методы** контроля обеспечивают наиболее точные результаты, так как они реализуются с помощью средств измерительной техники в местах контроля, прежде всего на границе контролируемой зоны. Так как измеряемые уровни опасных сигналов сравнимы с уровнями шумов, то для инструментального контроля необходимы высокочувствительные дорогостоящие измерительные приборы. Это обстоятельство существенно затрудняет реальные возможности проведения контроля.

Наибольшие проблемы возникают при инструментальном контроле ПЭМИН, так как частоты побочных излучений охватывают

практически весь радиодиапазон, а их уровни соизмеримы с электромагнитным фоном. Стандартная контрольно-измерительная аппаратура не обеспечивает проведение исследований ПЭМИН в необходимом объеме. Поэтому для этих целей используются дорогостоящие специальные приборы и приборы для физических научных исследований. Для измерений сигналов ПЭМИН применяются измерительные приемники, селективные микровольтметры и анализаторы спектра с техническими характеристиками:

- диапазон частот — десятки Гц–десятки ГГц;
- чувствительность — десятки–сотни нВ;
- динамический диапазон — 100–150 дБ;
- избирательность — единицы Гц–единицы МГц;
- точность измерения уровня сигнала — 1–2 дБ.

Так как многие сигналы ПЭМИН имеют импульсный характер и согласно требованиям нормативно-методических документов, эти приборы должны оснащаться пиковыми и квазипиковыми детекторами. Очень полезно для возможности автоматизации измерений наличие у измерительных приборов программно-аппаратного интерфейса с ПЭВМ. С целью комплексного решения проблем исследований ПЭМИН ведущие организации в области производства технических средств защиты информации «Нелк», «Иркос», «Маском», «Элерон» и др. выпускают постоянно совершенствуемые автоматизированные комплексы для измерений излучений ПЭМИН.

**Инструментально-расчетный** технический контроль позволяет снизить требования к параметрам измерительной техники. Эти методы предполагают проведение измерений не на границе контролируемой зоны, а вблизи возможных источников сигналов (ОТТС). Возле источников сигналов уровни сигналов выше и, соответственно, требования к чувствительности измерительных приборов ниже. Уровни же сигналов в местах проведения контроля рассчитываются по соответствующим методикам расчета. Так как в качестве исходных данных для расчета применяются результаты измерений, то точность контроля будет определяться точностью измерений и используемого математического аппарата.

Наконец, если отсутствуют требуемые для инструментального или инструментально-расчетного контроля измерительные при-

боры, то осуществляется **расчетный** технический контроль путем проведения расчетов по априорным или справочным исходным данным. Существующие методы расчетного технического контроля обеспечивают приемлемые для практики результаты при оценке угроз подслушивания и наблюдения. Для оценки этих угроз существует достаточно большой выбор данных в справочниках по акустике и оптике. Например, в справочнике по акустике приводятся данные об уровне громкости речи в помещении, величины звукоизоляции для различных ограждений, уровни акустических шумов для различных видов деятельности, по которым легко рассчитывается отношение сигнал/шум в точке контроля, например в коридоре или соседнем помещении.

Меры контроля, так же как и защиты, представляют совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по защите информации. Организационные меры контроля включают:

- проверку выполнения сотрудниками требований руководящих документов по защите информации;
- проверку работоспособности средств охраны и защиты информации от наблюдения, подслушивания, перехвата и утечки информации по материально-вещественному каналу (наличие занавесок, штор, жалюзей на окнах, чехлов на разрабатываемых изделиях, состояние звукоизоляции, экранов, средств подавления опасных сигналов и зашумления, емкостей для сбора отходов с демаскирующими веществами и т. д.);
- контроль за выполнением инструкций по защите информации о разрабатываемой продукции;
- оценку эффективности применяемых способов и средств защиты информации.

### Вопросы для самопроверки

1. Основные организационные меры по инженерно-технической защите информации.
2. Основные методы и средства инженерно-технической защиты информации от различных видов угроз.
3. Виды контроля эффективности инженерно-технической защиты информации.

4. Сущность постоянного контроля и его формы.
5. Виды технического контроля и когда они применяются?

### Основные положения раздела IV

1. Для защиты информации, содержащей государственную тайну, от технической разведки создана государственная систем защиты информации. Ее основными задачами являются:

- проведение единой технической политики, организация и координация работ по защите информации;
- противодействие технической разведки;
- создание и корректировка нормативно-правовой базы по защите информации;
- прогнозирование возможностей технической разведки;
- организация сил и создание средств защиты информации и ее контроля;
- контроль за состоянием защиты информации.

Пирамидальную структуру государственной системы образуют Межведомственная комиссия по защите государственной тайны, Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, федеральные органы, органы по защите информации федеральных ведомств, субъектов РФ, организаций и предприятий.

2. Межведомственная комиссия по защите государственной тайне подготавливает и представляет Президенту и Правительству РФ предложения по: организации разработке и выполнению государственных программ, нормативных и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне; правовому регулирования вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны; порядку определения размеров ущерба, который может быть нанесен безопасности России вследствие несанкционированного распространения секретных сведений; правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности.

Основным постоянно действующим федеральным органом государственной системы защиты информации от технической разведки является Федеральная служба по техническому и эк-

спортному контролю, в которую преобразована в марте 2004 г. Государственная техническая комиссия России. Задачи этой службы в основном соответствуют задачам государственной системы защиты информации. Координация работ в области защиты информации обеспечивается коллегией Федеральной службы по техническому и экспортному контролю, членами которых являются руководители ведомств, в которых решаются задачи по защите государственной тайны.

Федеральная служба безопасности РФ участвует в разработке, реализации и контроле мер по защите информации, содержащей государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности, обеспечивает криптографическую защиту информации, а также проводит лицензирование деятельности различных структур, связанной с государственной тайной, с разработкой ими средств информационной безопасности и услуг в этой сфере.

В министерствах, ведомствах, органах государственной власти субъектов Российской Федерации организуются Советы (Технические комиссии) и подразделения по защите информации. В отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, организующие и контролирующие деятельность в области оказания услуг по защите информации, органы сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы аттестации объектов информатизации.

В организациях и на предприятиях информацию защищают руководители, служба (подразделения) безопасности и сотрудники, работающие с информацией, содержащей государственную тайну. Типовая структура частной организации (предприятия) включает подразделение режима и охраны, специальный отдел, осуществляющий учет грифованных документов и образцов продукции, содержащих защищаемую информацию, подразделение инженерно-технической защиты информации и подразделение разведки и контрразведки.

3. Допуск предприятий (организаций, учреждений) к проведению работ, содержащих государственную тайну, созданию средств

защиты информации и оказанию услуг по защите государственной тайны возможен после получения ими лицензий на соответствующий вид деятельности. Лицензионная деятельность осуществляется Федеральной службой безопасности РФ и ее территориальными органами, Федеральной службой по техническому и экспортному контролю РФ, Службой внешней разведки РФ, Министерством обороны РФ (в пределах их компетентности). Лицензии выдаются на срок 3–5 лет на основании результатов специальных экспертиз предприятий, государственной аттестации их руководителей и выполнения условий, включающих соблюдения требований законодательных и иных нормативных актов РФ по обеспечению защиты государственной тайны, наличие в структуре предприятия специального подразделения и подготовленных сотрудников, наличия на предприятии соответствующих сертифицированных средств. Сертификацию средств проводят Федеральная служба по техническому и экспортному контролю РФ, ФСБ РФ, Служба внешней разведки РФ, аккредитованные органы по сертификации продукции, аккредитованные испытательные центры (лаборатории). Координация деятельности по сертификации возложена на Межведомственную комиссию по защите государственной тайны.

4. Деятельность системы защиты информации регламентируется документами, составляющую нормативно-правовую базу инженерно-технической защиты информации. Документы нормативно-правовой базы имеют трехуровневую структуру. Уровень государства представляют законы РФ, указы Президента РФ и постановления Правительства по вопросам защиты информации. Уровень ведомства образуют внутриведомственные и межведомственные документы. Документы организации и предприятия составляют соответствующий третий уровень. Документы более высокого уровня обязательны к исполнению на всех более низких уровнях.

По назначению документы делятся на руководящие, нормативные и методические. Руководящие документы определяют структуру органов безопасности, права и обязанности физических и юридических лиц, обеспечивающих защиту информации. В нормативных документах указываются значения различных показателей — нормативы, используемые для оценки возможностей средств добывания и эффективности защиты информации. В методических до-

кументах рассматриваются методики определения значений показателей добывания и защиты информации.

5. Основными руководящими документами, создаваемыми в организациях и на предприятиях, являются руководство (инструкция) по защите информации в организации (на предприятии), положение о службе безопасности в организации, инструкции по защите отдельных источников информации (изделиях и продукции). К основным нормативно-методическим документам относятся: перечень сведений, составляющих государственную (коммерческую) тайну, максимально допустимые значения уровней сигналов с защищаемой информацией и концентрации демаскирующих веществ на границах контролируемых зон, непревышение которых обеспечивает требуемый уровень безопасности информации, а также методики их измерения.

6. Меры по защите информации делятся на организационные и технические. Граница между ними достаточно условно определяется степенью использования технических средств. Организационные меры по инженерно-технической защите информации являются частью организационной защиты, основу которой составляют регламентация (установление временных, территориальных и режимных ограничений в работе людей и технических средств) и управление доступом к информации. Важнейшим направлением работ по защите информации является контроль эффективности защиты информации, проводимый силами службы безопасности, руководителями организации (учреждения, предприятия) и структурных организаций, всеми сотрудниками организации, допущенных к закрытой информации. Различают предварительный (после введенных изменений в систему защиты), периодический (систематический) и постоянный (по скрытым от проверяемых планам) контроль защиты информации.

К техническим относятся меры, реализуемые путем установки новых или модернизации используемых инженерных конструкций и технических средств защиты информации.

Эффективность защиты информации от технической разведки оценивается методами технического контроля. В ходе его производится определение технических параметров носителей информации. В результате сравнения их с нормативными значениями при-

нимается решение об уровне безопасности защищаемой информации. В зависимости от используемых для технического контроля средств применяют инструментальный, инструментально-расчетный и расчетный виды технического контроля.

## Литература к разделу IV


1. *Беляев Е. А., Лаврухин Ю. Н., Пицын В. В.* Государственная система защиты информации в Российской Федерации // Безопасность информационных технологий. — 2000. — № 3.
2. *Ярочкин В. И.* Система безопасности фирмы. — М.: Ось-89, 1997.
3. *Максимов Ю. Н., Сонников В. Г., Петров В. Г., Парашуткин А. В., Еремеев М. А.* Технические методы и средства защиты информации. — СПб.: Полигон, 2000.
4. *Журавленко Н. И., Курбанов Д. А.* Теория и методология защиты информации. Учебное пособие. — УФА: Оперативная полиграфия, 2001.
5. Инструкция о порядке проведения экспертиз предприятий, учреждений и организаций на право получения лицензии в области защиты информации. — М.: Гостехкомиссия России, 1998.
6. О лицензировании деятельности предприятий и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Постановление Правительства РФ от 15 апреля 1995 г. № 333.
7. Указ Президента РФ «О системе и структуре федеральных органов исполнительной власти» от 9 марта 2004 г. № 314.
8. Указ Президента РФ «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации» от 11 марта 2003 г. № 308.
9. Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Утверждена Директором ФСБ РФ 23 августа 1995 г. № 28.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации. — М.: Гостехкомиссия России, 1995.

# Раздел V. Методическое обеспечение инженерно-технической защиты информации

Методическое обеспечение включает комплекс методик и рекомендаций, обеспечивающих при их выполнении рациональный уровень инженерно-технической защиты информации. По существу эти методики должны для конкретных условий содержать ответы в виде алгоритмов, правил, рекомендаций на следующие вопросы:

- последовательность (алгоритм) работ по обеспечению инженерно-технической защиты на требуемом уровне;
- источники защищаемой информации, их характеристики, факторы, влияющие на безопасность содержащейся в них информации;
- угрозы безопасности информации, вероятность их реализации и причиняемый ими ущерб;
- рациональные меры, обеспечивающие требуемый уровень безопасности при минимальных затратах.

Кроме того, методическое обеспечение должно содержать математический аппарат для проведения необходимых оценок показателей в процессе оптимизации защиты.

## Глава 27. Рекомендации по моделированию системы инженерно-технической защиты информации

### 27.1. Алгоритм проектирования (совершенствования) системы защиты информации

Задача проектирования (разработки, совершенствования) системы защиты информации и ее элементов возникает тогда, когда создается новая организация с закрытой (секретной, конфиденциальной) информацией или существующая система не обеспечивает требуемый уровень безопасности информации.

Проектирование системы защиты, обеспечивающей достижение поставленных перед инженерно-технической защитой информации целей и решение задач, проводится путем системного анализа существующей и разработки вариантов требуемой. Построение новой системы или ее модернизация предполагает:

- определение источников защищаемой информации и описание факторов, влияющих на ее безопасность;
- выявление и моделирование угроз безопасности информации;
- определение слабых мест существующей системы защиты информации;
- выбор рациональных мер предотвращения угроз;
- сравнение вариантов по частным показателям и глобальному критерию, выбор одного или нескольких рациональных вариантов;
- обоснование выбранных вариантов в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

Так как отсутствуют формальные способы синтеза системы защиты, то ее оптимизация при проектировании возможна путем постепенного приближения к рациональному варианту в результате итераций.

Алгоритм проектирования системы защиты информации представлен на рис. 27.1.

Последовательность проектирования (модернизации) системы защиты включает три основных этапа:

- моделирование объектов защиты;
- моделирование угроз информации;
- выбор мер защиты.

Основным методом исследования систем защиты является моделирование. Моделирование предусматривает создание модели и ее исследование (анализ). Описание или физический аналог любого объекта, в том числе системы защиты информации и ее элементов, создаваемые для определения и исследования свойств объекта, представляют собой его **модель**. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

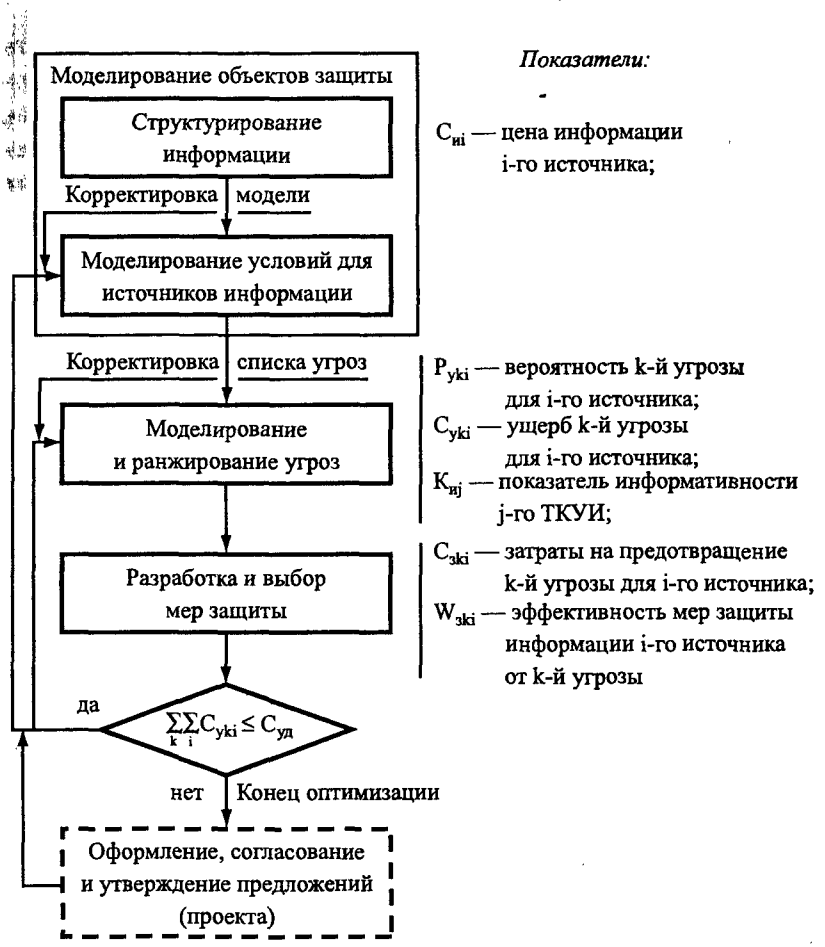



*Рис. 27.1.* Алгоритм проектирования системы защиты информации

Моделирование составляет основу деятельности живых существ, в том числе человека. В основе многих болезней психики человека лежат нарушения механизма моделирования окружающей среды. В крайних ее проявлениях в больном мозгу создаются модели, имеющие мало сходства с общепринятыми или объективно существующими моделями окружающего мира. В этом случае поступки больного человека на основе искаженной модели не соответствуют моделям других людей, а поведение такого челове-

ка классифицируется как ненормальное. Понятие «нормы» является достаточно условным и субъективным и может меняться в значительных пределах. Творческие люди способны в своем воображении создавать модели, отличающиеся от реальности, и эти модели в какой-то мере влияют на их поведение, которое иным людям кажется странным. Образ такого чудака-ученого Паганеля нарисовал Жюль Верн в своем романе «Дети капитана Гранта».

Так как основу жизни человека составляют химические и электрические процессы в его организме, то модели окружающей среды могут искажаться под действием химических наркотических веществ. Люди постоянно пользуются наркотиками, чтобы подкорректировать свои модели внешнего мира с целью уменьшить уровень отрицательных эмоций, возникающих при информационной недостаточности или несоответствии жизненных реалий задачам и целям человека. Наркотические вещества (алкоголь, табак, кофеин, кола), вызывающие слабое наркотическое воздействие на организм человека, узаконены. Другие — опиум, героин, ЛСД и т. д. столь губительны, что наркомания рассматривается человечеством как одна из наиболее страшных угроз его существованию.

Различают **вербальные, физические и математические модели** и соответствующее **моделирование**.

**Вербальная модель** описывает объект на национальном и профессиональном языках. Человек постоянно создает вербальные модели окружающей его среды и руководствуется ими при принятии решений. Чем точнее модель отображает мир, тем эффективнее при прочих равных условиях деятельность человека. На способности разных людей к адекватному моделированию окружающего мира влияют как природные (генетические) данные, так и воспитание, обучение, в том числе на основе собственного опыта, физическое и психическое состояния человека, а также мировоззренческие модели общества, в котором живет конкретный человек.

На естественном или профессиональном языке можно описать любой объект или явление. Сложные модели прошлой, настоящей или будущей жизни людей создают писатели. Но вербальные модели позволяют анализировать связи между ее элементами лишь на качественном уровне.

**Физическая модель** представляет материальный аналог реального объекта, который можно подвергать в ходе анализа раз-

личным воздействиям и получать количественные соотношения между этими воздействиями и результатами. Часто в качестве физических моделей исследуют уменьшенные копии крупных объектов, для изучения которых отсутствует инструментарий. Модели самолетов и автомобилей продувают в аэродинамических трубах, макеты домов для сейсмических районов испытывают на вибростендах и т. д. Но возможности физического моделирования объектов защиты и угроз ограничены, так как трудно и дорого создать физические аналоги реальных объектов. Действительно, для того чтобы получить физическую модель канала утечки, необходимо воспроизвести его элементы, в том числе среду, а также априори неизвестные средства и действия злоумышленника.

По мере развития вычислительной математики и техники расширяется сфера применения **математического моделирования**. Математическое моделирование предусматривает создание и исследование математических моделей реальных объектов и процессов. Математические модели могут разрабатываться в виде аналитических зависимостей выходов системы от входов, уравнений для моделирования динамических процессов в системе, статистических характеристик реакций системы на воздействия случайных факторов. Математическое моделирование позволяет наиболее экономно и глубоко исследовать сложные объекты, чего, в принципе, нельзя добиться с помощью вербального моделирования или что чрезмерно дорого при физическом моделировании. Возможности математического моделирования ограничиваются уровнем формализации описания объекта и степенью адекватности математических выражений реальным процессам в моделируемом объекте.

Подобные ограничения возникают при моделировании сложных систем, элементами которых являются люди. Многообразие поведения конкретного человека пока не поддается описанию на языке математических символов. Однако в статистическом смысле поведение человека более прогнозируемое и устойчивое.

Для моделирования сложных систем все шире применяется метод математического моделирования, называемый **имитационным моделированием**. Оно предполагает определение реакций модели системы на внешние воздействия, которые генерирует ЭВМ в виде случайных чисел. Статистические характеристики (математичес-

кое ожидание, дисперсия, вид и параметры распределения) этих случайных чисел должны с приемлемой точностью соответствовать характеристикам реальных воздействий. Функционирование системы при случайных внешних воздействиях описывается в виде алгоритма действий элементов системы и их характеристик в ответ на каждое воздействие на входе. Таким образом имитируется работа сложной системы в реальных условиях. Путем статистической обработки выходных результатов при достаточно большой выборке входных воздействий получаются достоверные оценки работы системы. Например, достаточно объективная оценка эффективности системы защиты информации при многообразии действий злоумышленников, которые с точки зрения службы безопасности носят случайный характер, возможна, как правило, на основе имитационного моделирования системы защиты.

Другое перспективное направление математического моделирования, которое представляет интерес для моделирования объектов защиты и угроз информации, — **компьютерные деловые игры**. Компьютерные деловые игры — аналог деловых игр людей, применяемый для решения проблем в организационных структурах. Деловая игра имитирует процесс принятия решения в сложных условиях недостаточности достоверной информации людьми, играющими роль определенных должностных лиц. Участниками компьютерной игры являются два человека или компьютер и человек. Причем за сотрудника службы выступает человек, а злоумышленника — компьютер или человек. Например, злоумышленник — компьютер устанавливает в случайном месте закладное устройство, а другой игрок — человек производит поиск закладного устройства с помощью различных выбранных средств по показаниям виртуальных приборов моделей этих средств.

Компьютерные игры по защите информации могут применяться как для анализа конкретных объектов, угроз и мер по защите, так и в качестве тренажеров для подготовки сотрудников службы безопасности.

В чистом виде каждый вид моделирования используется редко. Как правило, применяются комбинации вербального, физического и математического моделирования. С вербального моделирования начинается сам процесс моделирования, так как нельзя со-

здать физические или математические модели, не имея образного представления об объекте и его словесного описания. Если есть возможность исследовать свойства объекта на физической модели, то наиболее точные результаты обеспечиваются при физическом моделировании. Таким образом проверяют аэродинамику самолетов и автомобилей путем продувки уменьшенных физических моделей самолетов и автомобилей в аэродинамических трубах. Когда создание физической модели по тем или иным причинам невозможно или чрезмерно дорого, то проводят математическое моделирование, иногда дополняя его физическим моделированием отдельных узлов, деталей, т. е. тех частей объекта, описание которых не поддается формализации.

Так как создание и исследование универсальных (позволяющих проводить всесторонние исследования) моделей является достаточно дорогостоящим и трудным делом, то в целях упрощения моделей в них детализируют только элементы и связи между ними, необходимые для решения конкретной поставленной задачи. Остальные, менее существенные для решения конкретной задачи элементы и связи укрупняют или не учитывают вовсе. В результате такого подхода экономным путем исследуются с помощью дифференцированных моделей отдельные, интересующие исследователя, свойства объекта.

**Моделирование объектов защиты** предусматривает определение источников с защищаемой информацией и разработку моделей материальных объектов защиты. К объектам защиты относятся источники защищаемой информации и контролируемые зоны, в которых находятся эти источники.

В результате этого этапа определяются:

- модели объектов защиты с указанием всех источников информации с описанием факторов, влияющих на их безопасность;
- цена $C_{иi}$ защищаемой информации каждого i-го источника.

На основе полученных результатов на этапе **моделирования угроз** выявляются угрозы безопасности информации, производится оценка ожидаемого от их реализации потенциального ущерба и ранжирование угроз по потенциальному ущербу. При моделировании угроз определяются риск (вероятность) угрозы $P_у$ и ущерб $C_у$ в случае ее реализации. Знание ущерба позволяет также опреде-

лить количество угроз, нейтрализация которых обеспечит допустимый уровень безопасности информации $C_{уд}$. Для этого достаточно произвести последовательно сложение ущерба от угроз, начиная с последней в списке, и сравнить полученную сумму с допустимым ущербом. Черта под угрозами списка при условии приблизительного равенства суммарного ущерба от непредотвращенных угроз допустимому для владельца информации значению разделит список на 2 части. Верхняя, большая часть списка угроз включает угрозы, которые необходимо нейтрализовать для обеспечения допустимого уровня безопасности информации, нижняя — малосущественные угрозы.

Последовательность ранжированных угроз определяет последовательность **выбора мер защиты** на 3-м этапе. Этот этап начинается с определения мер защиты по нейтрализации первой, наиболее опасной угрозы, далее — второй угрозы и т. д. Если предотвращение угрозы в конце итерации достигается несколькими мерами, то вариант выбирается по критерию $W_{зкi}$ «эффективность-стоимость», т. е. из нескольких вариантов, обеспечивающих приблизительно равную безопасность, выбирается вариант с меньшими затратами. В качестве эффективности варианта наиболее часто используется отношение величины уменьшения ущерба при выбранной мере защиты к затратам на реализацию этого варианта. Из вариантов выбирается тот, для которого это отношение больше.

Для каждой выбранной меры защиты рассчитываются необходимые затраты на всем ее жизненном цикле (от ее реализации до прекращения). Если обозначить затраты на нейтрализацию к-й угрозы информации i-го источника через $C_{укi}$, то процедура выбора мер защиты условно завершается при выполнении условия $\sum_{k=1}\sum_{i=1} C_{укi} \geq C_{рз}$, где $C_{рз}$ — ресурс, выделяемый на защиту информации. Условность означает, что после выполнения этого условия целесообразно продолжить выбор с целью определения и оценки затрат для мер, использование которых превышает выделенный ресурс. Эти результаты позволят определить оставшиеся угрозы и необходимые для их нейтрализации дополнительные затраты.

Такой подход позволяет расходовать имеющийся ресурс на предотвращение наибольшего ущерба более эффективно, чем «раз-

мазывание» ресурса по всем угрозам, а во-вторых, знание конкретных непредотвращенных угроз позволяет владельцу информации сделать выбор: добавить ресурс или согласиться с оставшимся риском.

Выбором меры защиты, предотвращающей одну угрозу, завершается одна итерация проектирования системы защиты. После ее завершения в соответствии с указанной на рис. 27.1 обратной связью корректируются модели объектов защиты и угроз информации. Корректировка моделей объектов защиты заключается во внесении в них выбранных мер. Эти меры виртуально меняют защищенность информации и, соответственно, характеристики угроз ей. Кроме того, при корректировке список угроз сокращается сверху на единицу.

Целесообразность корректировки обусловлена связью между факторами, влияющими на безопасность информации, и угрозами. Например, предложение по установке для устранения угрозы информации путем подслушивания через приоткрытую дверь на ней доводчика одновременно снижает риск подсматривания.

Итерации продолжаются до достижения допустимого уровня безопасности или при превышении выделенного на защиту информации ресурса. При выполнении указанных условий процесс построения (совершенствования) требуемой системы завершается или продолжается с целью определения дополнительного ресурса.

После рассмотрения руководством предлагаемых вариантов (лучше двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы защиты или ее дополнительных элементов.

Следует подчеркнуть, что специалист по защите информации должен при обосновании предлагаемых руководству организации вариантов защиты учитывать психологию лица (руководителя), принимающего решение о реализации предложений, а также недостаточную информированность его об угрозах безопасности информации в организации.

Психологическим фактором, сдерживающим принятие решения руководителем о выделении достаточно больших ресурсов на защиту информации, является то обстоятельство, что в условиях скрытности добывания информации угрозы ей априори не представляются достаточно серьезными, а приобретают некоторый абстрактный характер. К существованию потенциальных угроз руководители привыкают и их не замечают так же, как люди не замечают множества угроз их здоровью. Кроме того, руководитель в силу собственного представления об угрозах, способах и средствах их нейтрализации может преувеличивать значимость одних мер защиты и приуменьшать другие. В результате этих обстоятельств мнение руководителя о необходимости и сущности мер защиты информации может не совпадать с предложениями специалистов по информационной безопасности. Однако такое несовпадение не должно уменьшать энтузиазм и настойчивость специалиста, так как оно характерно для любого вида деятельности, а умение обосновывать свои предложения является необходимым качеством любого специалиста.

Следует отметить, что рассмотренная последовательность в общем виде близка к существующим подходам. Например, процесс организации защиты в США в соответствии с концепцией «Opsec» (Operation Security) включает 7 этапов: от анализа объекта защиты на первом этапе до доведения персоналу фирмы мер по безопасности информации и осуществления контроля на последнем. Содержание ряда процедур метода «Opsec» близко рассмотренным. Однако в ней недостаточно места и внимания отведено моделированию угроз, а больше — анализу мер по защите информации руководящими лицами организации (фирмы, компании, учреждения).

## 27.2. Моделирование объектов защиты

Исходные данные для моделирования объектов защиты содержатся в перечнях сведений, содержащих семантическую и признаковую информацию и составляющих государственную или коммерческую тайну. Для организаций, независимо от формы собст-

венности, конкретный перечень сведений, составляющих государственную тайну, основывается на перечне сведений, отнесенных к государственной тайне в приложении Закона Российской Федерации «О государственной тайне» и на перечнях сведений заказывающего или выполняющего заказ ведомства. В коммерческих структурах перечень сведений, составляющих коммерческую тайну, определяется руководством организации. Перечни защищаемых демаскирующих признаков продукции разрабатываются при ее создании.

Источники защищаемой информации определяются путем ее структурирования. Можно предложить иные, более простые пути определения источников, например составить списки допущенных к закрытой информации должностных лиц, документов, продукции и других источников защищаемой информации. Однако такой способ определения источников информации не гарантирует полноту учета всех источников, требуемую системным подходом.

**Структурирование информации** представляет собой многоуровневый процесс детализации и конкретизации тематических вопросов перечней сведений. Например, тематический вопрос перечня сведений «перспективные разработки» на более нижнем уровне иерархии разделяется на «направления разработок», ниже — тематика, далее разработчики, документы и т. д. Процесс структурирования продолжается до уровня иерархии, информация на котором содержится в одном конкретном источнике (должностном лице, документе, продукции т. д.). Одни и те же источники могут содержать информацию разных тематических вопросов, а информация разных источников по некоторым тематическим вопросам может пересекаться.

Структурированная информация представляется в виде графа и таблицы. Нулевой (верхний) уровень графа соответствует понятию «защищаемая информация», а n-й (нижний) — информации одного источника из перечня источников организации. На основе графа разрабатывается таблица, вариант которой указан в табл. 27.1.

*Таблица 27.1*

| *№ источника информации* | *Наименование источника информации* | *Вид информации источника* | *Гриф секретности (конфиденциальности) информации* | *Цена информации* | *Контролируемая зона, в которой находится источник информации* |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| ..... | | | | | |
| | | | | | |

Порядковый номер элемента информации соответствует номеру тематического вопроса в структуре информации. Значность номера равна количеству уровней структуры, а каждая цифра — порядковому номеру тематического вопроса на рассматриваемом уровне среди вопросов, относящихся к одному тематическому вопросу на предыдущем уровне. Например, номер 2635 соответствует информации 5-го тематического вопроса на 4-м уровне, входящего в 3-й укрупненный вопрос 3-го уровня, который, в свою очередь, является частью 6-го тематического вопроса 2-го уровня, представляющего собой вопрос 2-й темы 1-го уровня.

Во 2-м столбце таблицы приводится наименование источника информации, а в 3–5 — характеристики содержащейся на них информации: вид, гриф и цена. В графе 6 указывается контролируемая зона, в которой может находиться (храниться, обрабатываться) защищаемая информация.

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая малогабаритная продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов. Крупногабаритная продукция размещается в складских помещениях или на открытых пространствах.

Источники информации в помещениях размещаются или отображаются:

- на столах помещения;
- в ящиках письменных столов помещения;
- в книжных шкафах помещения;

- в металлических шкафах помещений;
- в компьютерах;
- на экранах монитора и телевизора;
- на плакатах или экранах видеопроекторов, укрепляемых на стенах во время конференций, совещаний и других мероприятий по обсуждению вопросов с закрытой информацией.

Знание места расположения источника позволяет описать (смоделировать) условия обеспечения защиты информации. Задача моделирования источников информации состоит в объективном описании источников конфиденциальной информации в рамках существующей системы защиты.

Описание источников информации включает описание пространственного расположения источников информации и условий (факторов), влияющих на защищенность содержащейся в источниках информации (характеристик инженерных конструкций вокруг мест нахождения источников информации, радио- и электрооборудования, средств коммутации и др.).

Моделирование проводится на основе моделей контролируемых зон с указанием мест расположения источников защищаемой информации — планов помещений, этажей зданий, территории в целом. На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Так как подавляющее большинство источников информации размещаются в служебных помещениях, целесообразно результаты их обследования объединить в таблице, вариант которой приведен в табл. 27.2.

*Таблица 27.2*

| *1* | *2* | *3* | | |
|---|---|---|---|---|
| 1 | Название помещения | | | |
| 2 | Этаж | | Площадь, м$^2$ | |
| 3 | Количество окон, наличие штор на окнах | | Куда выходят окна | |

| 1 | 2 | 3 | | |
|---|---|---|---|---|
| 4 | Двери, кол-во, одинарные, двойные | | Куда выходят двери | |
| 5 | Соседние помещения, название, толщина стен | | | |
| 6 | Помещение над потолком, название, толщина перекрытий | | | |
| 7 | Помещение под полом, название, толщина перекрытий | | | |
| 8 | Вентиляционные отверстия, места размещения, размеры отверстий | | | |
| 9 | Батареи отопления, типы, куда выходят трубы | | | |
| 10 | Цепи электропитания | Напряжение, количество розеток электропитания, входящих и выходящих кабелей | | |
| 11 | Телефон | Типы, места установки телефонных аппаратов, тип кабеля | | |
| 12 | Радиотрансляция | Типы громкоговорителей места установки | | |
| 13 | Электрические часы | Тип, куда выходит кабель электрических часов | | |
| 14 | Бытовые радиосредства | Радиоприемники, телевизоры, аудио- и видеомагнитофоны, их количество и типы | | |
| 15 | Бытовые электроприборы | Вентиляторы и др., места их размещения | | |
| 16 | ПЭВМ | Количество, типы, состав, места размещения | | |

| 1 | 2 | 3 | |
|---|---|---|---|
| 17 | Технические средства охраны | Типы и места установки извещателей, зоны действий излучений | |
| 18 | Телевизионные средства наблюдения | Места установки, типы и зоны наблюдения телевизионных трубок | |
| 19 | Пожарная сигнализация | Типы извещателей, схемы соединения и вывода шлейфа | |
| 20 | Другие средства | | |

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения технических средств охраны, зоны наблюдения установленных телевизионных камер и т. д.

На плане территории организации отмечаются места нахождения здания (зданий), забора, КПП, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

Модель объектов защиты представляет собой набор чертежей, таблиц и комментарий к ним, содержащих следующие данные:

- полный перечень источников защищаемой информации с оценкой ее цены;
- описание характеристик, влияющих на защищенность содержащейся в них информации, мест размещения и нахождения ее источников;
- описание потенциальных источников опасных сигналов в местах нахождения источников информации.

На 1-м этапе не проводится оценка уровня защищенности источников информации. Данные моделирования объектов защиты

представляют собой лишь исходные данные для следующего этапа — моделирования угроз.

## 27.3. Моделирование угроз информации

Моделирование угроз безопасности информации предусматривает выявление угроз и их анализ с целью оценки возможного ущерба в случае их реализации. Определение значений показателей угроз информации представляет достаточно сложную задачу в силу следующих обстоятельств:

- добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации. Кроме того, следует иметь в виду, что характер и частота реализации угроз зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах, например, в странах с развитой рыночной экономикой не могут быть однозначно использованы для российских условий;
- оценка угроз информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;
- многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняет возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;
- априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Учитывая существенные различия процессов реализации угроз воздействия и утечки информации, моделирование угроз целесообразно разделить на:

- моделирование каналов несанкционированного доступа к защищаемой информации источников преднамеренных и случайных воздействий;
- моделирование технических каналов утечки информации.

### 27.3.1. Моделирование каналов несанкционированного доступа к информации

Из сил воздействия на носитель информации наибольшие угрозы могут создать злоумышленники и пожар. Они образуют каналы несанкционированного доступа к информации. Поэтому моделирование этих каналов предусматривает:

- моделирование каналов несанкционированного доступа злоумышленника к защищаемой информации;
- моделирование каналов несанкционированного доступа стихийных сил.

Действия злоумышленника по добыванию информации, так же как других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью. Так же как в криминалистике расследование преступления начинается с ответа на вопрос, кому это выгодно, так и при моделировании системы защиты необходимо, прежде всего, выяснить с максимально возможной достоверностью, кому нужна защищаемая информация.

Следует отметить, что прогнозирование источников угрозы информации является одним из основных условий ее эффективной защиты. При достаточно высокой достоверности прогноза создается запас времени для предотвращения угроз не только методами защиты источников, но и воздействия на источник угрозы. Например, можно договориться с конкурентом или, при наличии фактов его противоправных действий, потребовать от него их прекращения под угрозой предания гласности фактов нарушений.

Источники угрозы информации можно условно разделить на 4 группы:

- сотрудники (агенты) зарубежных спецслужб;
- конкуренты на рынке и в борьбе за власть;
- криминальные элементы;
- сотрудники организации, пытающиеся добыть и продать информацию по собственной инициативе или завербованные зарубежной разведкой, конкурентом или криминалом.

Сотрудники спецслужб (агенты) характеризуются высокой профессиональностью и технической оснащенностью. Оперативно-

технические характеристики используемых ими технических средств часто превосходят характеристики средств, имеющихся на рынке.

Руководители коммерческих структур привлекают для добывания информации о своих конкурентах уволившихся сотрудников силовых ведомств и используют имеющиеся на рынке технические средства. В среднем квалификация этих злоумышленников и возможности применяемых ими технических средств ниже.

Криминал привлекает для решения рассматриваемых задач или уволенных за низкие моральные качества и правонарушения, или уволившихся «обиженных» бывших сотрудников спецслужб. Квалификация этих злоумышленников, как правило, достаточно высокая, а используемые ими технические средства присутствуют на рынке. Однако если спецслужбы и конкуренты проводят разведывательную операцию скрытно, то криминал может пойти на силовое проникновение с использованием стрелкового оружия и взрывчатых веществ.

Слабая квалификация сотрудников организации частично компенсируется возможностью более простого проникновения их к источнику информации. Завербованный сотрудник организации может получить инструкции по маршруту и способам проникновения, необходимые технические средства или деньги на их приобретение.

В зависимости от квалификации, способов подготовки и проникновения в организацию злоумышленников разделяют на следующие типы:

- **неквалифицированный**, который ограничивается внешним осмотром объекта, проникает в организацию через двери и окна;
- **малоквалифицированный**, изучающий систему охраны объекта и готовящий несколько вариантов проникновения, в том числе путем взлома инженерных конструкций;
- **высококвалифицированный**, который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы и маршруты проникновения и отхода.

Моделирование угроз информации с учетом квалификации злоумышленника обеспечивает экономию ресурса на защиту информации в том случае, если удается с достаточно большой досто-

верностью определить источник угрозы. В противном случае во избежание грубых ошибок в условиях отсутствия информации о злоумышленнике, его квалификации и технической оснащенности лучше переоценить угрозу, чем ее недооценить, хотя такой подход и может привести к увеличению затрат на защиту. В этом случае целесообразен при моделировании угроз информации следующий подход к формированию модели злоумышленника:

- злоумышленник представляет серьезного противника, тщательно готовящего операцию по добыванию информации;
- он изучает обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;
- намечает варианты и проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи;
- имеет в распоряжении современные технические средства проникновения и преодоления механических преград.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны.

Для создания модели угрозы физического проникновения, достаточно близкой к реальной, необходимо «перевоплотиться» в злоумышленника и смоделировать операцию проникновения за него. Для моделирования угроз целесообразно привлекать в качестве «злоумышленников» опытных сотрудников службы безопасности, не участвующих в моделировании объектов охраны и допущенных к обобщенной информации о способах и средствах охраны организации. Использование в качестве экспертов сотрудников других структурных подразделений недопустимо, так как это может привести к утечке ценной информации. «Злоумышленник» должен выявить на основе данных 1-го этапа организации защиты «слабые места» в существующей системе охраны и определить возможные маршруты его движения к месту нахождения источника.

Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели.

Маршруты движения обозначаются на соответствующих планах модели объектов охраны. Так как моделирование основывается на случайных событиях, то целесообразно наметить несколько вариантов проникновения.

Основными элементами путей проникновения могут быть:

- естественные (ворота, двери КПП);
- вспомогательные (окна, люки, коммуникационные каналы, тунели, пожарные лестницы);
- специально создаваемые (проломы, подкопы, лазы).

Варианты проникновения могут также существенно отличаться и проводиться:

- скрытно или открыто;
- без использования или с использованием специальных приспособлений;
- без использования или с использованием силовых методов нейтрализации охраны.

Возможность реализации угрозы проникновения злоумышленника к источнику информации оценивается произведением вероятностей двух зависимых событий: безусловной вероятностью попытки к проникновению и условной вероятностью преодоления им всех рубежей на пути движения его от точки проникновения до места непосредственного контакта с источником информации — вероятностью проникновения.

Вероятность попытки добыть информацию, в том числе путем проникновения к источнику, зависит от соотношения цены добытой информации и затрат злоумышленника на ее добывание. Вероятность принятия злоумышленником решения на проникновение близка к нулю, если цена информации меньше или соизмерима с затратами на ее приобретение. При превышении цены над затратами эта вероятность возрастает. Так как вероятность не может превысить 1, то зависимость вероятности попытки несанкционированного доступа злоумышленника от соотношения цены информации $C_{ци}$ над затратами $C_{зз}$ можно аппроксимировать выражениями: $P_{ву} = 0$ при условии $C_{ци} / C_{зз} < 1$ и $P_{ву} = 1 - \exp(1 - \alpha_{ву} C_{ци} / C_{зз})$, если $C_{ци} / C_{зз} > 1$, где $\alpha_{ву}$ — коэффициент, учитывающий степень роста зависимости вероятности $P_{ву}$ от соотношения $C_{ци} / C_{зз}$.

Такая математическая модель достаточно хорошо согласуется с логикой принятия решения злоумышленником на осуществление операции по добыванию информации. Действительно, когда $C_{ци} \le C_{зз}$, то $P_{ву} \approx 0$, затем при увеличении этого соотношения более 1 вероятность попытки проникновения сначала медленно, а затем более существенно возрастает, а при существенном росте соотношение цены и затрат монотонно приближается к 1.

Вероятность проникновения к источнику информации при условии принятия решения злоумышленником на проведение операции (возникновения угрозы) зависит от уровня защищенности источника информации, времени реакции сил нейтрализации, квалификации злоумышленника и его технической оснащенности. В интегральном виде эта вероятность определяется вероятностями обнаружения $P_{оз}$ и необнаружения $P_{нз}$ вторжения злоумышленника системой защиты информации и соотношением времени задержки злоумышленника $\tau_{зз}$ и времени реакции системы защиты $\tau_{рс}$. Так как при $\tau_{зз} << \tau_{рс}$ вероятность проникновения близка к 1, а при противоположном соотношении времен близка к 0, то вероятность проникновения злоумышленника $P_{пз}$ в первом приближении удобно аппроксимировать экспоненциальной функцией $P_{пз} = P_{нз} + P_{оз}\exp(-\beta_{пз}\tau_{зз} / \tau_{рс})$, где $\beta_{пз}$ — коэффициент, учитывающий уровень защищенности организации.

С учетом этих моделей вероятность угрозы воздействия можно оценить по формуле:

$$P_{ув} = P_{ву} \cdot P_{пз} = [1 - \exp(-\alpha_{ву}C_{ци} / C_{зз})][P_{нз} + P_{оз}\exp(-\beta_{пз}\tau_{зз} / \tau_{рс})]$$

при $C_{ци} / C_{рр} > 1$.

Более точные результаты могут быть получены в результате моделирования проникновения. Для моделирования проникновения целесообразно использовать аппарат видоизмененных семантических сетей. Семантическая сеть представляет собой граф, узел которого соответствует одному из рубежей и одной из контролируемых зон организации, а ребро — вероятности и времени перехода источника угрозы из одного рубежа (зоны) в другой (другую). Для наглядности целесообразно узел — рубеж представить в виде кружка, а узел — зону — в виде прямоугольника. В свою очередь рубеж и зона могут находиться в разных состояниях. Рубеж мо-

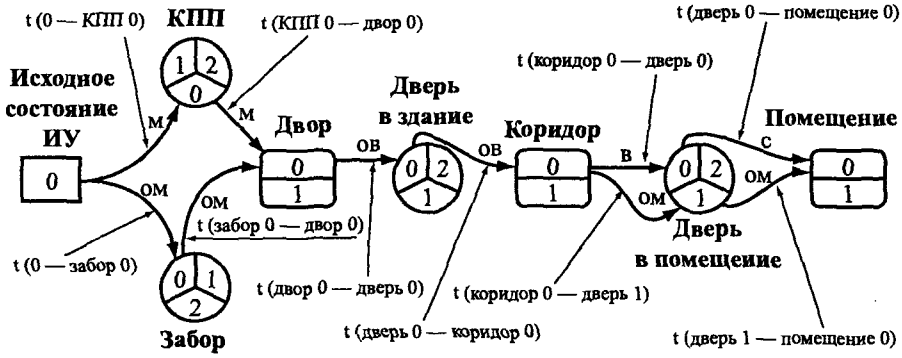



*Рис. 27.2.* Математическая модель проникновения злоумышленника к источнику информации

*Обозначения*: ИУ — источник угроз;
м — малая;
ом — очень малая;
в — высокая;
с — средняя;
ов — очень высокая вероятность;
t (КПП0 — двор 0) — время задержки при движении из КПП с 0 состоянием до двора с нулевым состоянием и т. д.

жет быть открытым (состояние 0), закрытым без включения технических сигнализации (состояние 1) и закрытым с включенными средствами сигнализации (состояние 2). Например, дверь в рабочее время может быть открытой или закрытой, во внерабочее время — закрытой с подключением охранной сигнализации. Зона как часть пространства с контролируемым уровнем безопасности может быть свободной для прохода и проезда (состояние 0) и закрытой (с включенными средствами охраны) — состояние 1. Пример моделей каналов несанкционированного доступа источника угрозы в выделенное помещение показан на рис. 27.2.

Как следует из рисунка, существует множество путей перехода из нулевого состояния в конечное с разными вероятностями и временами задержками. Каждый путь характеризуется значениями вероятности и времени проникновения. Вероятность проникновения по i-му пути равна произведению вероятностей всех n промежуточных переходов по этому пути. Время задержки равно сумме задержек на каждом переходе. Чем выше вероятность и меньше время, тем выше величина угрозы.

Учитывая, что злоумышленник будет выбирать путь с лучшими для решения своей задачи параметрами — с большей вероятностью и меньшим временем проникновения, то угрозы ранжируются по этим параметрам. Если один из путей имеет большую вероятность, но меньшее время проникновения, то при ранжировании возникнет проблема выбора. Для ее решения необходимо два показателя свести к одному. В качестве такого глобального показателя можно использовать не имеющее физического смысла отношение времени задержки и вероятности проникновения по рассматриваемому участку пути. Для такого критерия наибольшую угрозу представляет путь проникновения с меньшими значениями интегрального показателя.

Возможные пути проникновения злоумышленников отмечаются линиями на планах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в таблицу, вариант которой указан в табл. 27.3.

*Таблица 27.3*

| № источника информации | Цена информации источника | Путь источника угрозы | Характеристика угрозы | | Величина ущерба | Ранг угрозы |
|---|---|---|---|---|---|---|
| | | | риск проникновения | время проникновения | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| ..... | | | | | | |
| | | | | | | |

*Примечание.* Под источником угрозы понимается злоумышленник и пожар.

### 27.3.2. Моделирование каналов утечки информации

Обнаружение и распознавание технических каналов утечки информации, так же как любых объектов, производится по их демаскирующим признакам. В качестве достаточно общих признаков или индикаторов каналов утечки информации могут служить указанные в табл. 27.4.

*Таблица 27.4*

| Вид канала | Индикаторы |
|---|---|
| 1 | 2 |
| Оптический | Просматриваемость помещений из окон противоположных домов.<br>Близость к окнам деревьев.<br>Отсутствие на окнах занавесок, штор, жалюзей.<br>Просматриваемость содержания документов на столах со сторон окон, дверей, шкафов в помещении.<br>Просматриваемость содержания плакатов на стенах помещения для совещания из окон и дверей.<br>Малое расстояние между столами сотрудников в помещении.<br>Просматриваемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников.<br>Складирование продукции во дворе без навесов.<br>Малая высота забора и дырки в нем. |

| 1 | 2 |
|---|---|
| | Переноска и перевозка образцов продукции в открытом виде.<br>Появление возле территории организации (предприятия) посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино- и видеокамерами. |
| Радиоэлектронный | Наличие в помещении радиоэлектронных средств, ПЭВМ, ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов.<br>Близость к жилым домам и зданиям иных организаций.<br>Использование в помещении средств радиосвязи.<br>Параллельная прокладка кабелей в одном жгуте при разводке их внутри здания и на территории организации.<br>Отсутствие заземления радио- и электрических приборов.<br>Длительная и частая парковка возле организации чужих автомобилей, в особенности с сидящими в машине людьми. |
| Акустический | Малая толщина дверей и стен помещения<br>Наличие в помещении открытых вентиляционных отверстий<br>Отсутствие экранов на отопительных батареях<br>Близость окон к улице и ее домам.<br>Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами.<br>Частая и продолжительная парковка возле организации чужих автомобилей. |
| Вещественный | Отсутствие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами.<br>Применение радиоактивных веществ.<br>Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов.<br>Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги. |

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки. В конкретных условиях их состав существенно больший.

Потенциальные каналы утечки определяются для каждого источника информации, причем их количество может не ограничи-

ваться одним или двумя. Например, от источника информации — руководителя фирмы, работающего в своем кабинете, утечка информации возможна по следующим каналам:

- через дверь в приемную или коридор;
- через окно на улицу или во двор;
- через вентиляционное отверстие в соседние помещения;
- с опасными сигналами по радиоканалу;
- с опасными сигналами по кабелям, выходящим из помещения;
- по трубам отопления в другие помещения здания;
- через стены, потолок и пол в соседние помещения;
- с помощью закладных устройств за территорию фирмы.

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. В основном применяются вербальные и математические модели. Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала канала является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;
- канал утечки включает разнообразные инженерные конструкции (бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздать которые на макетах невозможно или требуются огромные расходы.

Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют **структурная** и **пространственная** модели. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приемника сигналов, удаленность их от границ территории организации, ориентация вектора распространения носителя информации в канале утечки информации и ее протяженность. Структурную модель канала целе-

сообразно представлять в табличной форме, пространственную — в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Структурная и пространственная модели не являются автономными, а взаимно дополняют друг друга.

Динамику канала утечки информации описывают **функциональная** и **информационная** модели. Функциональная модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а информационная содержат характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

Указанные модели объединяются и увязываются между собой в рамках **комплексной модели** канала утечки. В ней указываются интегральные параметры канала утечки информации: источник информации и ее вид, источник сигнала, среда распространения и ее протяженность, место размещения приемника сигнала, риск канала и величина потенциального ущерба. Каждый вид канала содержит свой набор показателей источника и приемника сигналов в канале, позволяющих оценить длину технического канала утечки информации и показатели возможностей органов государственной и коммерческой разведки.

Так как приемник сигнала является принадлежностью злоумышленника и точное место его размещения и характеристики не известны, то моделирование канала проводится применительно к гипотетическому приемнику. В качестве приемника целесообразно рассматривать приемник, параметры которого соответствуют современному уровню, а место размещения выбрано рационально. Уважительное отношение к интеллекту и техническим возможностям противника гарантирует от крупных ошибок в значительно большей степени, чем пренебрежительное.

При описании приемника сигнала необходимо учитывать реальные возможности злоумышленника. Очевидно, что приемники сигналов коммерческой разведки не могут, например, размещаться на космических аппаратах. Что касается технических характеристик средств добывания, то они для государственной и коммерчес-

кой разведки существенно не отличаются. Расположение приемника злоумышленника можно приблизительно определить исходя из условий обеспечения значения отношения сигнал/помеха на входе приемника, необходимого для съема информации с допустимым качеством, и безопасности злоумышленника или его аппаратуры.

Если возможное место размещения приемника сигналов выбрано, то в ходе моделирования канала рассчитывается энергетика носителя на входе приемника с учетом мощности носителя на выходе источника, затухания его в среде распространения, уровня помех, характеристик сигнала и его приемника.

Все выявленные потенциальные каналы утечки информации и их характеристики записываются в табл. 27.5.

*Таблица 27.5*

| *Источник информации* | *Путь утечки информации* | *Вид канала* | *Длина канала* | *Риск утечки* | *Величина ущерба* | *Ранг угрозы* |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| ... | ... | ... | ... | ... | ... | ... |
| | | | | | | |

В графе 2 указываются основные элементы канала утечки информации (источника сигналов, среды распространения и возможные места размещения приемника сигналов). По физической природе носителя определяется вид канала утечки информации, который указывается в столбце 3. По расстоянию между источником сигнала (информации) и приемником сигнала (получателя) определяется длина канала, значение которой вписывается в графу столбца 4. Риск утечки информации (столбец 5) по рассматриваемому каналу оценивается близостью параметров канала и сигнала на входе его приемника к нормативным значениям, при которых риск (вероятность) утечки ниже допустимого значения. Он зависит от совокупности факторов, влияющих на характеристики канала утечки: разрешающей способности приемника сигналов, их энергетики, вероятности выполнения временного условия разведывательного контакта средства добывания с источником инфор-

мации. В зависимости, например, от принадлежности противоположного дома к жилому или административному, из окна которого возможно в принципе наблюдение за объектом защиты, существенно различаются оценки реальности использования этого оптического потенциального канала утечки для добывания информации. Если дом жилой, то злоумышленнику под видом сотрудника спецслужбы или за деньги проще договориться с жильцами о снятии на определенное время комнаты, чем с руководством организации. При определении реальности канала следует учитывать степень выполнения временного и энергетического условий разведывательного контакта с источником информации. Для обеспечения временного контакта надо или знать время проявления демаскирующих признаков объекта или наблюдение должно вестись непрерывно в течение, например, рабочего дня. Для выполнения энергетического условия разведывательного контакта необходимо, чтобы длина канала была больше расстояния от источника информации до злоумышленника или его приемника сигнала.

Моделирование угроз безопасности информации завершается их ранжированием в табл. 27.5.

На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала. Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например по виду, положению в пространстве, способам и средствам защиты, угрозам.

### *27.3.2.1. Методические рекомендации по оценке угроз оптических каналов утечки информации*

На риск утечки информации по оптическим каналам утечки информации влияет, прежде всего, количество и точность измерения видовых демаскирующих признаков объектов наблюдения, передаваемых по этим каналам. В свою очередь количество признаков и точность их измерения зависят от количества пикселей изображения объекта на сетчатке глаза, фотопленке или мишени ПЗС-матрицы оптического приемника. Чем из большего количества точек состоит изображение, тем большее количество признаков наблюдается на изображении объекта и с большей точностью они могут быть измерены. Количество точек определяется размерами объекта, дальностью наблюдения и разрешающей способностью средств наблюдения. Линейные размеры объекта и дальность наблюдения интегрально характеризуются угловыми размерами по горизонтали и вертикали объекта $\alpha_{ог}$ и $\alpha_{ов}$. Если угловая разрешающая способность средства наблюдения по горизонтали и вертикали равны $\beta_{сг}$ и $\beta_{св}$ соответственно, то количество точек изображения составит $N = \alpha_{ог}\alpha_{ов} / \beta_{ог}\beta_{ов}$.

В существующих методиках вероятность обнаружения и распознавания объектов наблюдения в видимом диапазоне света учитывают большое количество факторов: контраст объекта по отношению к фону, линейные размеры объекта, его периметр, площадь, коэффициент, учитывающий форму объекта, расстояние от средства наблюдения до объекта, прозрачность среды распространения, характеристики средства наблюдения (фокусное расстояние и разрешающую способность).

Однако используемые для оценки вероятности обнаружения и распознавания объектов наблюдения параметры являются вторичными по отношению к количеству пикселей изображения. Действительно, для изображения любой формы существует минимальное количество пикселей, при котором еще можно определить форму. При меньшем количестве пикселей отличить, например, круг от квадрата невозможно. Зависимость вероятности правильного определения формы простого объекта от количества точек изображения, укладывающихся на критическом размере объекта, приведена на рис. 27.3 [1].

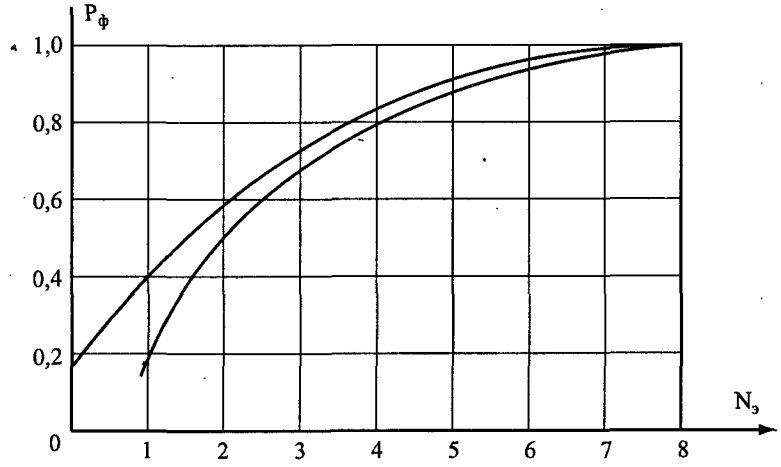



*Рис. 27.3.* Зависимость вероятности обнаружения объекта простой формы от количества пикселей

*Примечание.* Простой объект имеет круглую, квадратную, прямоугольную, треугольную и другую простые формы. Под критическим размером объекта понимают минимальный размер проекции объекта на плоскость, перпендикулярную линии визирования средства наблюдения.

Разброс значений обусловлен отличиями методик разных авторов. Как следует из этого рисунка и других данных, вероятность распознавания формы объекта без помех по его изображению, образуемому из более чем 7–8 точек по горизонтали и вертикали, приближается к 1. Действительно, безошибочно распознаются цифры и буквы текста, напечатанного 9 игольчатым принтером. По усредненным данным минимальное количество точек изображения, обеспечивающее вероятность 0,9 обнаружения (распознавания) объекта простой формы, образуют матрицу из (5–6) × (5–6) точек.

Зависимость вероятности обнаружения объекта от количества пикселей в его изображении по вертикали или горизонтали в первом приближении можно аппроксимировать экспоненциальной функцией вида $P_o = 1 - \exp(-\alpha N_{в(г)})$, где $\alpha = 0{,}25$ — нормирующий коэффициент, определяемый из условия: для обнаружения (распоз-

навания) сложного объекта с вероятностью 0,9 необходимо около 9 точек по горизонтали и вертикали.

Количество пикселей, содержащееся в изображении объекта наблюдения, можно оценить по формуле линзы, иллюстрируемой рис. 27.4.

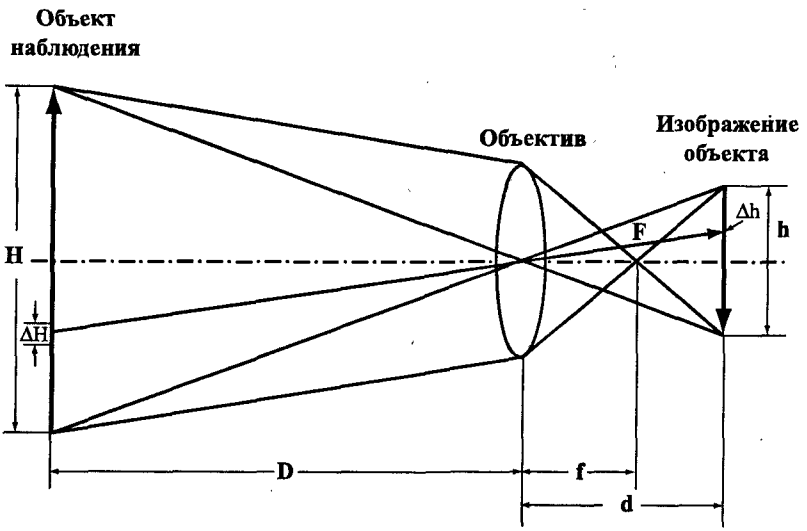



*Рис. 27.4.* Схема наблюдения объекта

На рисунке объект высотой H создает изображение высотой h. Точка изображения размером Δh соответствует элементу объекта размером ΔH. Объект расположен на удалении D от объектива средства наблюдения. Объектив с фокусным расстоянием f на удалении d формирует изображение объекта. В общем случае $d \neq f$. Величины D, d и f связаны формулой линзы: $\frac{1}{D}+\frac{1}{d}=\frac{1}{f}$. Так как $D >> d$, то $d \approx f$. При этом условии выполняется равенство $\frac{H}{D}=\frac{h}{f}$, из которого следует, что $h = Hf / D$. Количество пикселей, укладывающихся в размер h, равно hR, где R — разрешающая способность средства наблюдения в лин/мм. Разрешающая способность средства наблюдения рассчитывается как среднегеометрическая сумма разрешающих способностей объектива $R_о$ и светочувствительного элемента $R_э$, т. е. $R = \frac{R_о R_э}{R_о + R_э}$. Окончательно, количество пиксе-

лей N в h определяется как $N = RHf / D$. Пиксель же изображения соответствует участку объекта размером $\Delta H = D / Rf$.

После подстановки значения N в приведенную ранее формулу она приобретает вид: $P_o = 1 - \exp(-0{,}25RHf / D)$. Так как риск утечки информации определяется, прежде всего, вероятностью обнаружения объектов, то в соответствии с этой формулой риск утечки информации по оптическому каналу повышается с увеличением линейного размера объекта, разрешающей способности средства наблюдения и фокусного расстояния его объектива, а уменьшается с увеличением длины канала. Например, риск утечки информации при фотографировании лица человека на удалении 100 м фотоаппаратом с $R_o = 50$ лин/мм, $R_э = 100$ лин/мм, длиннофокусным объективом ($f = 30$ см) составляет около 0,53. Для указанных исходных данных вероятность прочтения текста документов стандартного формата А4 нулевая, но распознавание текста и рисунков на листах формата А1 (плакатах) достаточно большая.

Разрешающая способность оптико-электронных средств наблюдения (цифровых фотоаппаратов, видео- и телевизионных камер), использующих в качестве светочувствительных элементов ПЗС-матрицы, чаще оценивается количеством телевизионных строк кадра или пикселей, из которых формируется изображение наблюдаемого пространства. Эти характеристики оптико-электронных средств наблюдения достаточно просто преобразовать в лин/мм, разделив число строк или пикселей по вертикали на размеры ПЗС матрицы применяемого средства наблюдения. Например, эквивалентное разрешение телевизионной камеры отечественного стандарта в 625 ТВС, использующей 1/3 дюймовую ПЗС-матрицу (3,6 × 4,8 мм), достигает 160–180 лин/мм. Разрешающая способность приборов ночного видения хуже и составляет 40–60 лин/мм.

Вероятность обнаружения и распознавания объектов наблюдения характеризует риск утечки информации по оптическому каналу.

### *27.3.2.2. Методические рекомендации по оценке угроз акустических каналов утечки информации*

Защищенность речевой информации оценивается энергетическими и информационными показателями. Как известно, в качестве **энергетического показателя** защищенности речевой информации

используется отношение сигнал/шум на входе акустического приемника. Так как в общем случае спектры речи и помехи не совпадают, то для гарантированного превышения спектральных составляющих помехи над всеми спектральными составляющими речи необходимо значительное превышение средних уровней помехи над средним уровнем речи. Понимание речи невозможно, если отношение помеха/сигнал равно 6–8, а акустический сигнал не воспринимается человеком как речевой, если отношение помеха/сигнал превышает 8–10. Для гарантированной защищенности речевой информации отношение сигнал/шум должно быть не более 0,1 или (–10) дБ.

Для оценки значения энергетического показателя применяются следующие методы:

- инструментальный контроль;
- инструментально-расчетный;
- расчетный.

а) Инструментальный контроль предусматривает измерение уровней акустических сигналов в зоне подслушивания, прежде всего, на границе контролируемой зоны. В качестве измерительных приборов используются акустические спектральные анализаторы (спектроанализатора) и шумомеры. На вход спектрального анализатора подается электрический сигнал от микрофона или акселерометра (при измерении уровня структурного звука). Спектроанализаторы бывают последовательные и параллельные, аналоговые и цифровые.

Последовательные спектроанализаторы применяются для измерения характеристик стационарных процессов путем последовательной перестройки его селективных элементов. Для измерения кратковременных акустических сигналов используют параллельные спектроанализаторы. Типовой параллельный спектроанализатор состоит из предварительного и входного усилителей, аттенюатора и n каналов, перекрывающих весь звуковой диапазон. Каждый канал включает октавный фильтр, детектор, интегратор и запоминающее устройство, с выхода которого сигнал подается на устройство отображения — экран монитора. На нем наблюдается спектр (уровни спектральных составляющих в октавной полосе) входного акустического сигнала.

Шумомер представляет собой упрощенный вариант последовательного акустического спектроанализатора с встроенным микрофоном и стрелочной или цифровой индикацией уровня сигнала. Аналоговые спектроанализаторы вытесняются цифровыми спектроанализаторами, в которых аналоговый входной сигнал преобразуется в цифровой аналого-цифровым преобразователем. Цифровая обработка сигнала предоставляет более широкие возможности и высокие точности измерения акустических сигналов.

Учитывая, что современные звуковые карты компьютеров содержат достаточно качественные стереофонические усилители (стереоусилителя) и аналогово-цифровые преобразователи (АЦП), компьютер с соответствующим программным обеспечением может использоваться в качестве прибора для инструментального контроля затухания среды потенциального акустического канала утечки информации. Разместив микрофон одного канала в месте нахождения источника речевого сигнала, а микрофон другого канала — в месте возможного нахождения средства злоумышленника, можно определить коэффициенты затухания среды распространения в октавных полосах как отношение уровней соответствующих сигналов на выходе каналов стереоусилителя. С целью исключения влияния несимметричности характеристик микрофонов, каналов стереоусилителя и АЦП звуковой карты измерения проводятся для двух вариантов размещения микрофонов. В ходе второго измерения микрофоны меняются местами, а результаты измерений усредняются.

б) При наличии измерительных приборов с ограниченными возможностями, позволяющими проводить только отдельные измерения, например измерять уровни громкости исходного речевого сигнала, применяют инструментально-расчетные методы контроля. Получение итоговых результатов обеспечивается по известным математическим формулам с получением недостающих данных из справочников.

в) Расчетный контроль безопасности акустической информации обеспечивается в результате проведения расчетов по известным формулам с использованием справочных данных.

Если громкость речи в помещении равна $L_и$, а звукоизоляция среды на пути распространения звука — $Q_с$, то громкость речи в точке подслушивания человеком $L_п = L_и - Q_с$ (рис. 27.5).

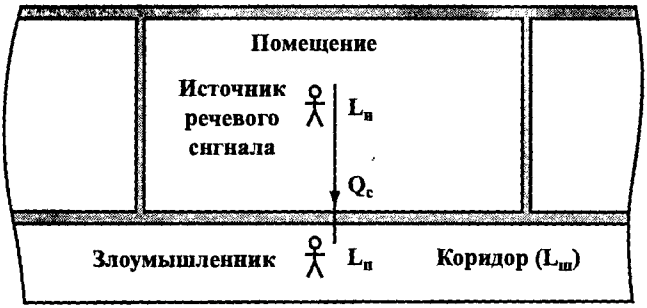



*Рис. 27.5.* Схема подслушивания речи в коридоре

Если подслушивание проводится с использованием технических средств с частотной коррекцией, компенсирующей снижение чувствительности слуха человека в области низких частот на 6 дБ, то уровень громкости в коридоре определяется по уточненному выражению $L_п = L_и - Q_с + 6$.

На возможности подслушивания речи влияют акустические шумы, создаваемые на улице и в здании. Усредненные уровни шумов в помещении на частоте 1000 Гц указаны в табл. 27.6.

*Таблица 27.6*

| *№ п/п* | *Характеристика помещения* | *Громкость шума, дБ* |
|---|---|---|
| 1 | Кабинет при одном работающем | 20–25 |
| 2 | Тихая комната | 25–30 |
| 3 | Бухгалтерия без посетителей | 30–35 |
| 4 | Коридоры | 35–40 |
| 5 | Комната шумная | 40–50 |
| 6 | Шумное собранне | 65–70 |

Уровень сигнала с учетом акустических шумов $L_ш$ в точке подслушивания $L_п = L_и - Q_с - L_ш$. По этим выражениям легко оценивается возможность подслушивания в смежном помещении или в коридоре. Например, если громкость источника речи в помещении составляет 60 дБ, звукоизоляция гипсобетонной стены толщиной 80 мм, отделяющей помещение от коридора, равна 41 дБ, а уровень шума — 30 дБ, то отношение сигнал/шум речевого сигнала в кори-

доре составит менее (–10) дБ и, следовательно, речь не слышна. Но если громкость повысится до 70 дБ, то отношение сигнал/шум увеличится до 1, при котором речь становится различимой.

Приведенная методика является упрощенной, не учитывающей неравномерность спектров речевого сигнала и шума, размеры и неоднородность звукоизолирующего ограждения, а также амплитудно-частотные характеристики среды и уха. Ухо человека имеет максимальную чувствительность в области нескольких кГц, которая ухудшается на низких и высоких частотах. Характеристики спектра речи, шума и среды указаны в табл. 27.7.

*Таблица 27.7*

| *№ п/п* | *Характеристики элементов акустического канала утечки информации* | *Уровни сигналов и их затухание в дБ в октавных полосах со средней геометрической частотой в Гц* | | | | | |
|---|---|---|---|---|---|---|---|
| | | *250* | *500* | *1000* | *2000* | *4000* | *8000* |
| 1 | Речь при средней громкости 70 дБ | 70 | 67 | 62 | 57 | 53 | 49 |
| 2 | Шум при средней громкости 40 дБ | 40 | 34 | 30 | 27 | 25 | 23 |
| 3 | Звукоизоляция гипсобетонной стены толщиной 80 мм | 33 | 39 | 47 | 54 | 60 | 60 |

Более точные аналитические зависимости учитывают размеры и структуру звукоизолирующего ограждения. Звукоизоляция неоднородной поверхности, состоящей из элементов с разной звукоизоляцией, площадью S определяется по формуле [3]:

$$Q_{нп} = Q_c - 10\lg\left[1 + \frac{S_o}{S_c + S_o}(10^{0,1(Q_c - Q_o)} - 1)\right],$$

где $Q_c$ и $Q_o$ — величина звукоизоляции стены и окна (двери) соответственно; $S_c$ и $S_o$ — площадь стены и окна (двери) соответственно.

В качестве **информационного критерия** используется **разборчивость речи**. В зависимости от рассматриваемого элемента речи различают формантную, слоговую, словесную и фразовую разборчивость речи. Если количество элементов речи рассматривать как

косвенную меру информации на выходе и входе акустического канала утечки, то разборчивость речи характеризует относительную пропускную способность акустического канала утечки.

**Формантная разборчивость** речи характеризует разборчивость наименьших элементов речи — звуков или фонем. В русском языке фонем больше, чем букв (40–41 фонем, 32 буквы), так как многим буквам соответствуют 2 звука, например мягкие и твердые звуки одинаковых букв. Звуки речи имеют неравномерный спектр. Области спектра, в которых сосредоточена энергия звука, называются **формантами**. Форманты звуков речи заполняют ее частотный диапазон 15–7000 Гц. Каждая форманта вносит определенный вклад в разборчивость речи. С целью оценки формантной разборчивости частотный диапазон разбивают на 20 полос равной разборчивости. Если обозначить через $К_{фi}$ коэффициент разборчивости форманты в i-й полосе равной разборчивости, то формантная разборчивость определяется как «взвешенная» сумма разборчивости формант: $А_ф = 0{,}05 \sum_{i=1}^{20} К_{фi}$.

Значение коэффициента разборчивости форманты в i-й полосе зависит от субъективного уровня ощущения формант $Е_ф = В_ф - В_п$, где $В_ф$ и $В_п$ — средние спектральные значения уровней речевого сигнала и помех в полосе равной разборчивости, в дБ. Связь между значениями $Е_ф$ и $К_ф$ иллюстрируется данными табл. 27.8.

*Таблица 27.8*

| $Е_ф$ | $К_ф$ | $Е_ф$ | $К_ф$ | $Е_ф$ | $К_ф$ |
|---|---|---|---|---|---|
| –12 | 0,010 | –1 | 0,17 | 22 | 0,900 |
| –11 | 0,015 | 0 | 0,20 | 23 | 0,915 |
| –10 | 0,020 | 3 | 0,30 | 24 | 0,030 |
| –9 | 0,030 | 6 | 0,40 | 25 | 0,945 |
| –8 | 0,040 | 9 | 0,50 | 26 | 0,960 |
| –7 | 0,050 | 12 | 0,60 | 27 | 0,970 |
| –6 | 0,060 | 15 | 0,70 | 28 | 0,980 |
| –5 | 0,075 | 18 | 0,80 | 29 | 0,985 |
| –4 | 0,095 | 19 | 0,83 | 30 | 0,990 |
| –3 | 0,110 | 20 | 0,86 | 33 | 0,995 |
| –2 | 0,140 | 21 | 0,88 | 36 | 1,000 |

Как следует из данных таблицы, разборчивость приближается к нулевому значению (речь не воспринимается) при $E_ф < -10 - (-12)$ дБ, что соответствует отношению помеха/сигнал менее 10.

Так как полосы равной разборчивости неравномерные и не совпадают у разных людей и, следовательно, возникают большие проблемы при их определении, то на практике диапазон речевого сигнала делят на 6 октавных полос. Граничные значения соседних октавных полос отличаются в 2 раза и воспринимаются человеком как равноудаленные, Среднегеометрические частоты октавных полос, охватывающие речевой диапазон, имеют значения 250, 500, 1000, 2000, 4000 и 8000 Гц. Форманты каждой октавной полосы в отличие от полос равной разборчивости вносят разный вклад в формантную разборчивость речи (см. табл. 27.9).

*Таблица 27.9*

| Среднегеометрическая частота октавной полосы, Гц | 250 | 500 | 1000 | 2000 | 4000 | 8000 |
|---|---|---|---|---|---|---|
| Вклад октавной полосы в формантную разборчивость речи, % | 6,7 | 12,5 | 21,2 | 29,4 | 25 | 5,2 |

Наибольший вклад в разборчивость речи вносят форманты в диапазоне частот стандартного телефонного канала 300–4000 Гц, что и позволило сузить стандартный телефонный канал до диапазона 300–3400 Гц. С учетом вклада каждой октавной полосы формантная разборчивость вычисляется по формуле:

$$A_ф = 0{,}067w_1 + 0{,}125w_2 + 0{,}212w_3 + 0{,}294w_4 + 0{,}25w_5 + 0{,}052w_6,$$

где $w_i$ — разборчивость речи в i-й октавной полосе.

**Слоговая, словесная и фразовая разборчивость** определяется в результате артикуляционных измерений. В ходе этих измерений отобранные (не имеющие дефектов речи и имеющие хороший слух) и предварительно тренированные люди — артикулянты размещаются в местах, соответствующих границам исследуемого канала связи или утечки информации. Один участник (артикулянт) читает слоги, слова или фразы специальных артикуляционных таблиц, другой участник измерения записывает услышанные элементы речи. Путем сравнения переданных и принятых элементов речи рассчитывается соответствующая разборчивость как процент

правильно понятых. Слоги, слова и фразы артикуляционных таблиц подбираются из условия отсутствия между ними корреляционных связей, которые повышают условную вероятность распознавания элементов речи после приема предшествующих.

Для обеспечения гарантированной защиты речевой информации по информационному критерию разборчивость речи в месте подслушивания должна быть меньше предельно допустимой в 1,5-2 раза.

Между значениями разборчивости и отношения сигнал/шум существует однозначная связь. Чем больше отношение сигнал/шум тем выше разборчивость. По значению отношения сигнал/шум определяют разборчивость, а по разборчивости — понятность речи. Чем выше понятность речи, тем большую угрозу создает акустический канал утечки информации. В первом приближении можно каждому значению градации понятности речи поставить в соответствие качественное значение риска утечки: отличная понятность → очень большой риск утечки, хорошая понятность → большой риск, удовлетворительная понятность → средний риск, предельно допустимая понятность → малый риск, отсутствие понятности → очень малый риск.

Физическое моделирование акустического канала утечки информации можно осуществить путем непосредственного или с помощью технических средств подслушивания речи, имитируемой с помощью аудиомагнитофона в помещении в условиях малых акустических помех, например после работы в вечернее время. Если при соответствующей громкости речи источника информации понятность речи в местах возможного нахождения акустического приемника злоумышленника ниже предельно допустимой, то безопасность речевой информации обеспечивается. В противном случае необходимо принимать меры по дополнительной звукоизоляции источника речевого сигнала.

### *27.3.2.3. Методические рекомендации по оценке угроз радиоэлектронных каналов утечки информации*

Утечка информации возможна по радиоканалу и проводам. Условия предотвращения утечки по радиоэлектронному каналу:

- напряженность электромагнитного поля на границе контролируемой зоны меньше нормативного значения;

- напряжение электрического тока в линии (цепях электропитания) на границе контролируемой зоны менее нормированного значения.

**а) Оценка утечки информации по радиоканалу**

Источниками радиосигналов с речевой информацией, циркулирующей в помещении, являются:

- передающие устройства закладных устройств;
- источники побочных электромагнитных излучений.

Напряженность электромагнитного поля на границе контролируемой зоны зависит от:

- мощности источника радиоизлучений;
- характера изменения напряженности электромагнитного поля при его распространении от источника излучения к приемнику сигналов;
- величины затухания энергии поля в среде распространения до границы контролируемой зоны;
- расстояния источника излучения до границы контролируемой зоны.

1) Мощность передатчиков закладных устройств колеблется в широких пределах: от единиц мВт до единиц Вт. Максимальная дальность распространения радиосигналов оценивается по формуле:

$$D \le \frac{\lambda}{4\pi}\sqrt{\frac{P_{ис} G_{ис} G_{пр} \gamma_{п}}{P_{пр} q_{пр}}},$$

где $P_{ис}$ — мощность источника (передатчика); $P_{пр}$ — предельная чувствительность приемника; $G_{ис}$ и $G_{пр}$ — коэффициенты усиления антенн передатчика и приемника; $\gamma_{п}$ — коэффициент, учитывающий несовпадение углов поляризации передающей и приемной антенн; $q_{пр}$ — отношение сигнал/шум на входе приемника, при котором обеспечивается требуемое качество информации на его выходе.

**Пример**. Для закладного устройства с $P_{ис} = 10$ мВт и $G_{ис} = 0{,}05$, приемника с $P_{пр} = 10^{-13}$ Вт, $G_{пр} = 0{,}1$ и $q_{пр} = 10$, а также для $\gamma_{пр} = 0{,}5$ и $\lambda = 6$ м ($f = 500$ МГц) $D \le 2500$ м (без учета затухания электромагнитной волны в среде распространения и внешних помех).

Электромагнитная волна из помещения затухает, в основном, в элементах здания (табл. 27.10) [3].

*Таблица 27.10*

| *Тип здания* | *Ослабление радиосигнала в дБ на частоте* | | |
|---|---|---|---|
| | *100 МГц* | *500 МГц* | *1 ГГц* |
| Деревянное здание с толщиной стен 20 см | 5–7 | 7–9 | 9–11 |
| Кирпичное здание с толщиной стен в 1,5 кирпича | 13–15 | 15–17 | 16–19 |
| Железобетонное здание с ячейкой арматуры 15 × 15 см и толщиной 16 см | 20–25 | 18–19 | 15–17 |

*Примечание.* В рассматриваемых зданиях 30% площади занимают оконные проемы.

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, соизмеримая с размерами ячеек арматуры.

При ослаблении электромагнитной волны стенами здания на 20 дБ дальность ее распространения уменьшается на 1 порядок. Для рассмотренного примера она составит единицы сотен и десятки метров.

2) Оценка угрозы утечки информации, вызванной побочными излучениями ОТСС и ВТСС, производится путем сравнения радиусов зон потенциального перехвата опасных радиосигналов с размерами контролируемых зон организации. В качестве критерия применяется энергетический критерий — уровень поля или электрического сигнала.

Различают 2 вида зон (см. рис. 27.6):

- зона 1 с радиусом $R_1$ — пространство вокруг ОТСС, в пределах которого не допускается размещение ВТСС, через которое может происходить утечка информации за пределы контролируемой зоны;
- зона 2 с радиусом $R_2$, в пределах которой уровень сигнала, излучаемого ОТСС, превышает норматив.

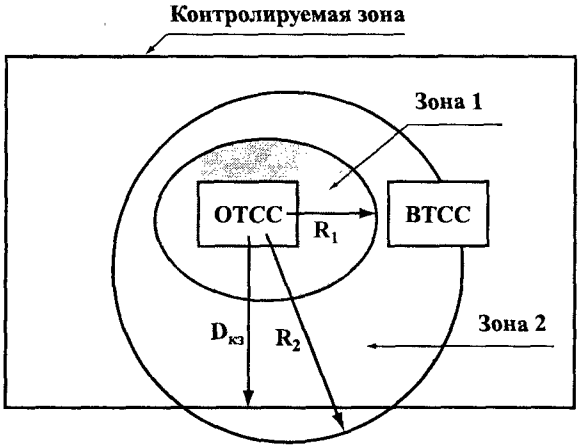



*Рис. 27.6.* Зоны безопасности информации

Так как диаграмма направленности вокруг источника излучения, как правило, неравномерная, то радиусы определяются на направлениях максимальной напряженности сигнала.

Информация, содержащаяся в информационных параметрах радиосигналов, защищена вне пределов контролируемой зоны, если $R_{з2} < D_{кз}$, а $R_{з1}$ меньше расстояния между ОТСС и ВТСС. Здесь $D_{кз}$ — расстояние от ОТСС до границы контролируемой зоны.

Радиус зоны 2 больше радиуса зоны 1, так как в качестве средства перехвата используется специальный приемник с существенно более высокими характеристиками, чем ВТСС.

Для оценки уровня защищенности необходимо оценить радиусы зон 1 и 2. Для этого определяется характер изменения напряженности поля от расстояния до источника излучения. Как известно, этот характер зависит от того, в какой зоне (ближней или дальней) производится измерение.

В общем случае напряженность поля изменяется в виде $E(H) = E_0(H_0) / r^q_{1,2}$, где $q = 1, 2, 3$. Характер изменения оценивается в результате измерения напряженности E в двух точках (см. рис. 27.7).

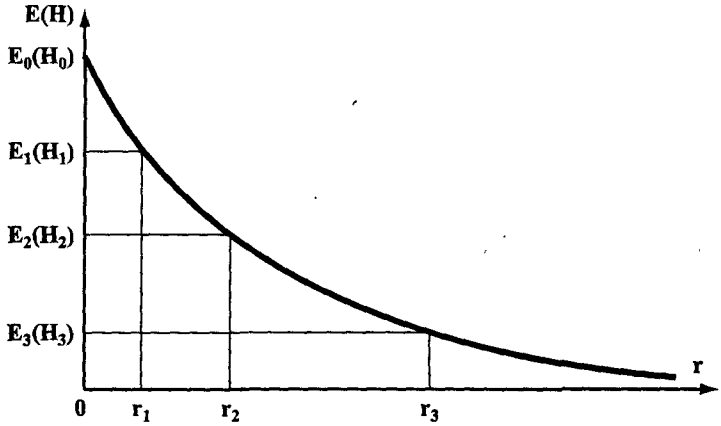



*Рис. 27.7.* Зависимость напряженности электрического (магнитного) полей от расстояния до их источников

Измерив E(H) в двух точках, можно приближенно оценить показатель q степени изменения напряженности полей по формуле:

$$q = \frac{\ln(E_1 / E_2)}{\ln(r_1 / r_2)}.$$

По значению q определяются размеры зоны 2:

$$R_{з2} = r_1 \sqrt[q]{E_1(H_1) / E_н(H_н)}.$$

Более точная аппроксимация $E(H) = f(r)$ обеспечивается по трем точкам: $E(H) = x/r^3 + y/r^2 + z/r$. Неизвестные x, y и z определяются из системы линейных уравнений:

$$\begin{cases} \dfrac{x}{r_1^3} + \dfrac{y}{r_1^2} + \dfrac{z}{r_1} = E_1(H_1), \\ \dfrac{x}{r_2^3} + \dfrac{y}{r_2^2} + \dfrac{z}{r_2} = E_2(H_2), \\ \dfrac{x}{r_3^3} + \dfrac{y}{r_3^2} + \dfrac{z}{r_3} = E_3(H_3). \end{cases}$$

В результате решения этой системы уравнений по правилу Крамера

$$x = \frac{r_1 r_2 r_3 \left[ E_1 r_1^2 (r_2 - r_3) + E_2 r_2^2 (r_3 - r_2) + E_3 r_3^2 (r_1 - r_2) \right]}{w},$$

$$y = \frac{E_1 r_1^3 (r_3^2 - r_2^2) + E_2 r_2^3 (r_1^2 - r_3^2) + E_3 r_3^3 (r_2^2 - r_1^2)}{w},$$

$$z = \frac{E_1 r_1^3 (r_2 - r_3) + E_2 r_2^3 (r_3 - r_1) + E_3 r_3^3 (r_1 - r_2)}{w},$$

$$w = r_1^2 r_2 - r_1 r_2^2 + r_1 r_3^2 + r_2^2 r_3 - r_2 r_3^2.$$

Допустимые напряженности полей $E_н$ и $H_н$ указываются в нормативно-методических документах для разных категорий помещений.

Нормативные значения напряженности поля с защищаемой информацией определяются из соотношения $E_н = E_ш \delta_н$, где $E_ш$ — напряженность электрического поля шумов, $\delta_н$ — нормативное (максимальное) отношение сигнал/шум, при котором обеспечивается безопасность информации. Так как уровень шумов приемника зависит от его полосы пропускания $\Delta f$, то вводят такой показатель, как уровень $E_{шн}$ нормированного шума (приведенный к единице полосы). С учетом этого $E_ш = E_{шн} \cdot \sqrt{\Delta f}$.

**б) Оценка угрозы утечки речевой информации по проводам**

Источниками опасных сигналов в проводах являются:

- ЭДС, наводимые электромагнитными полями в проводах;
- сигналы случайных акустоэлектрических преобразователей.

Эквивалентная схема цепи, содержащей источник опасных сигналов $U_и$, приведена на рис. 27.8.

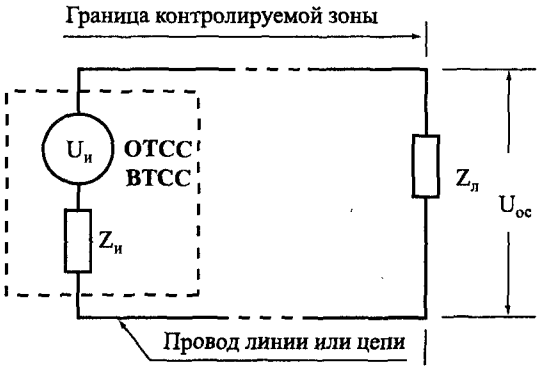



*Рис. 27.8.* Эквивалентная схема проводной линии

Напряжение опасного сигнала $U_{ос}$ в линии (проводных цепях) на границе контролируемой зоны равно величине $U_{ос} = \frac{U_и Z_л}{Z_и + Z_л}$, где $Z_и$ и $Z_л$ — комплексные сопротивления источника опасных сигналов и линии соответственно.

Безопасность речевой информации обеспечивается от утечки по проводным линиям при выполнении условия $U_{ос} < U_н$, где $U_н$ — нормативное значение опасного сигнала.

Если источником опасных сигналов во ВТСС являются поля ОТСС напряженностью Е, то $U_и = E \cdot h_д$, где $h_д$ — действующая высота случайной антенны технического средства. Действующая высота $h_д$ ВТСС, расположенного в помещении, измеряется как расстояние от середины высоты ВТСС до середины перекрытия пола. Воздействие электрического поля на ОТСС на ВТСС осуществляется через паразитную емкостную связь с $Z_и \approx 1 / \omega C_и$. Если принять $U_{ос} = U_и$, то собственную емкость ВТСС измеряют методом замещения. С этой целью ВТСС замещают моделью (шаром или диском) с известной емкостью С и измеряют индуцируемое в ней напряжение $U_э$. Емкость ВТСС оценивается по формуле: $C_и = C_э \cdot U_и / U_э$, где $U_и$ — напряжение, индуцируемое во ВТСС.

### *27.3.2.4. Методические рекомендации по оценке угроз вещественных каналов утечки информации*

Уровень угрозы вещественного канала зависит от вида информации и ее носителя. Так как отходы производства, содержащие защищаемую информацию, создаются сотрудниками организа-

ции (предприятия), то на цену этой информации косвенно влияет должностной (научный) статус сотрудника — автора отходов. Цена информации в черновике диктуемого руководителем документа в общем случае выше, чем черновик рядового исполнителя. Так как основные меры защиты информации от утечки по вещественному каналу относятся к организационным, то значения показателей этого канала зависят от пунктуальности выполнения мер защиты. Нарушения режима работы организации или технологии производства новой продукции, содержащей защищаемую информацию, увеличивают риск утечки информации по этому каналу.

Определить в общем случае количественные значения риска утечки на основе инструментальных измерений в вещественном канале невозможно. Однако можно качественно оценить потенциальную угрозу в результате анализа реальности возможных нарушений режима и технологии. В качестве таких нарушений, например, могут рассматриваться факты, отмеченные в актах предыдущих проверок уровня безопасности информации. Кроме того, в любой системе существуют слабые места, уровень защиты которых трудно поддается контролю. Например, требования о необходимости записи по вопросам закрытой информации только в учтенных тетрадях или на учтенных листах сотрудниками организации далеко не всегда выполняются неукоснительно, а обеспечить непрерывный контроль за всеми сотрудниками невозможно. Поэтому существует, хотя и малый, риск утечки информации за счет нарушений этих требований.

## 27.4. Методические рекомендации по оценке значений показателей моделирования

Одной из наиболее трудных задач, возникающих в процессе моделирования, является определение значений показателей: цены информации, уровня угрозы и вероятности ее реализации, затрат на предотвращение угроз. Такая проблема возникает при решении любых слабоформализуемых задач. Поэтому ей уделяется постоянное внимание, хотя до ее решения еще далеко. Отсутствие однозначной зависимости результата решения слабоформализуемой задачи от исходных данных, их неопределенность и недостоверность существенно затрудняют использование традиционного математи-

ческого аппарата. Более того, часто этого не следует делать, так как при недостоверных исходных данных можно получить результат, далекий от реального.

Так как люди в повседневной жизни решают слабоформализуемые задачи чаще, чем точные, то в процессе эволюции создан механизм их решения с приемлемой для выживания homo sapies точностью. Алгоритм их решения на бессознательном уровне пока не известен, но получены полезные эвристические рекомендации.

Так как решение слабоформализуемых задач производит человек, в дальнейшем — лицо, принимающее решение (ЛПР), то используемые методы объективно должны основываться на способностях и возможностях ЛПР по решению таких задач. Они учитывают следующие эмпирические положения:

- точность решения ЛПР слабоформализуемых задач обратно пропорциональна их сложности, причем ЛПР может в среднем оперировать одновременно с 5–9 понятиями;
- объективность оценок ЛПР показателей процедур решения слабоформализуемых задач в условиях недостаточной и недостоверной информации выше при использования им качественных шкал, чем количественных;
- при ограниченности ресурса его целесообразно использовать, прежде всего, для предотвращения угроз с максимальным ущербом;
- эффективность использования ресурса выше при его комплексном применении, когда одни и те же меры предотвращают несколько угроз.

Из этих достаточно общих положений следует, что для повышения точности и объективности ЛПР выбора, целесообразно:

- детализировать алгоритм решения слабоформализуемой задачи, разбивая его на этапы и процедуры, при определении показателя которых возникает меньше ошибок;
- при оценке показателей отдельных этапов и процедур использовать качественные шкалы с числом градаций (значений) в пределах 5–9;
- проранжировать угрозы безопасности информации по потенциальному ущербу и расходование ресурса на предотвращение уг-

роз производить последовательно, начиная с мер предотвращения угрозы с максимальным ущербом;

- при разработке мер защиты учитывать влияние предыдущих мер на снижение ущерба рассматриваемой угрозы.

Действительно, если человек не знает точного количественного значения какого-либо показателя, он заменяет его качественной мерой: высокий человек, большая цена, длинный путь, малая вероятность и др. При этом его качественные оценки могут весьма точными и однозначными.

В настоящее время предпринимаются многочисленные попытки использовать для обработки нечетко определенной информации аппарат нечетких множеств Заде [5]. Суть подхода Заде состоит в замене качественных понятий, например, таких как «цена информации, «угроза безопасности информации» и др., названных лингвистическими переменными, на количественные аналоги и последующей обработке числовой информации с помощью предложенного Заде математического аппарата. С этой целью вводятся функции принадлежности или совместимости количественных значений лингвистической переменной. На рис. 27.9 в графической форме представлены функции принадлежности $\mu_в(h)$ лингвистических переменных «высокая женщина» и «высокий мужчина».

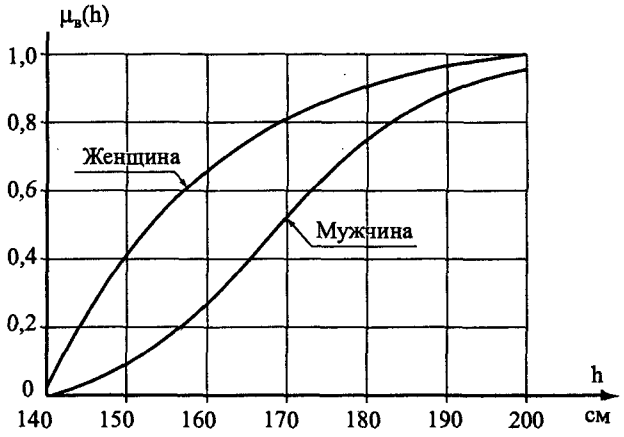



*Рис. 27.9.* Графическое представление функции принадлежности

На этом рисунке по оси абсцисс указаны значения роста человека в см, а по оси ординат — числа в интервале [0–1], соответствующие степени принадлежности значения роста женщины или мужчины лингвистической переменной «высокий(ая)».

Функции принадлежности могут быть определены в графической или табличной форме, а также в виде алгебраической суммы значений $\mu_в(h)$. Например, функция принадлежности лингвистической переменной «высокий мужчина», графическое представление которой приведено на рис. 27.9, имеет вид:

$$\mu_{вм} = 0/140 + 0{,}1/150 + 0{,}3/160 + 0{,}53/170 + 0{,}75/190 + 0{,}95/200.$$

Каждое слагаемое этой функции соответствует значению функции принадлежности для определенного значения роста человека.

Предложенный в теории нечетких множеств математический аппарат в виде операций сложения, объединения, умножения позволяет производить обработку цифрового массива функций принадлежности. Несмотря на привлекательность аппарата нечетких множеств при его применении возникают проблемы, прежде всего, психологического плана, которые сдерживают его внедрение. Суть этих проблем состоит в том, что в ходе обработки функций принадлежности получаются результаты в виде числовых матриц, трудно поддающиеся осмысленному обратному преобразованию в значения лингвистических переменных.

Для оценки показателей предлагается аппарат, который лучше согласуется с логикой человека, оперирующий качественными понятиями. Он основывается как на понятиях аппарата нечетких множеств, так и психологических основах обработки информации человеком. Принципы его иллюстрируются рис. 27.10.

Суть предложений состоит в следующем.

1. Человек принимает решения путем сравнительного анализа небольшого количества альтернативных вариантов, в среднем около 7. Альтернативы оцениваются качественными значениями порядковой или ранговой шкалы, или в терминологии Заде — термами лингвистической переменной. Учитывая способность человека одновременно оперировать в среднем 5–9 словами и числами, количество градаций лингвистической шкалы следует выбирать такого же порядка.

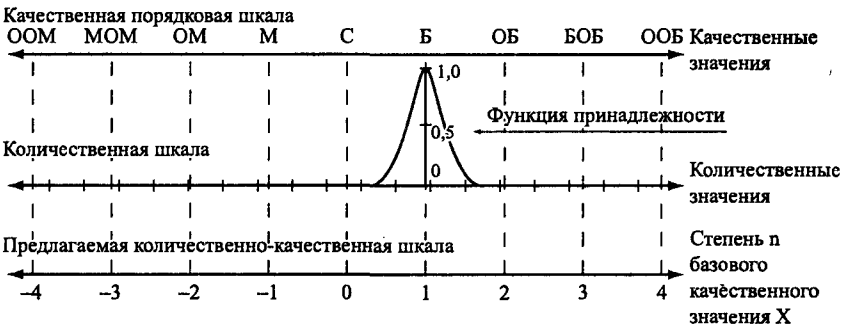



*Рис. 27.10.* Шкалы для оценки показателей в области информационной безопасности

*Обозначения*: ООМ — очень, очень малый(ая); МОМ — менее чем очень малый; ОМ — очень малый; М — малый; С — средний; Б — большой; ОБ — очень большой; БОБ — более чем очень большой; ООБ — очень, очень большой.

2. Значения лингвистических переменных «цена информации», «риск угрозы», «ущерб от реализации угрозы»: очень очень большая, очень большая, большая, средняя, малая, очень малая, очень очень малая лингвистических переменных образуют качественную шкалу с 7 градациями. Для других лингвистических переменных градации шкалы будут характеризоваться другими понятиями. Но общими для них являются базовые значения «большой(ая)», «малый(ая)» и модификаторы «очень».

3. Над качественной шкалой располагается количественная шкала, значения которой соответствуют значениям показателя качественной шкалы. Значения «большой» или «малый» идентичны этим значения в первой степени, т. е. большой = большой$^1$, а малый = малый$^1$.

4. Учитывая способность человека к дихотомии (разбиению линейного размера пополам), точка отсчета (условный нуль) соответствует значению «средний (средняя)» лингвистической переменной качественной шкалы или 0 количественной шкалы. Значение «средний» можно интерпретировать как «не большой и не малый», «не высокий и не низкий». Примем, что средний соответствует большому или малому в нулевой степени, т. е. средний = большой$^0$ = малый$^0$.

5. Справа от нуля располагается подмножество больших значений лингвистических переменных с базовым значением «большой» («высокий»). Другие большие значения образуются с помощью модификаторов «очень»: очень большой, очень, очень большой (чрезмерно большой) и т. д. Психологически модификатор «очень» соответствует концентрации значения лингвистической переменной путем возведения ее в степень 2. Следовательно, очень большой = большой$^2$; очень, очень большой = (очень большой)$^2$ = большой$^4$.

6. Слева от нуля находится область подмножества малых значений лингвистической переменной или отрицательных чисел количественной шкалы. Значения лингвистической переменной, меньшие «среднего», соответствуют «малый», «очень малый» и т. д. или «низкий», «очень низкий» и т. д. Учитывая, что психологически произведение «большой» на «малый» воспринимается как «средний», то малый = средний / большой» = болшой$^0$ / большой$^1$ = большой$^{-1}$, очень малый = большой $^{-2}$ и т. д.

Следовательно, все значения лингвистической переменной можно выразить через одно базовое значение «большой», «малый», «высокий», «низкий» в соответствующей степени.

С учетом введенных обозначений любая лингвистическая переменная может быть записана в виде алгебраического выражения: $yx^n$, где y — наименование лингвистической переменной (цена, вероятность, риск, ущерб и др.), x — базовое значение лингвистической переменной, n — положительные или отрицательные натуральные числа. Например, показатель «очень большая цена информации» = $x^2y$, где x — большая, y — цена информации.

Для повышения объективности оценки показателей необходимо выявить факторы, влияющие на их величину, и установить связи между значениями этих факторов и показателей. Основные из этих факторов указаны в табл. 27.11.

*Таблица 27.11*

| *№ п/п* | *Лингвистическая переменная (показатель процедур оптимизации)* | *Условные обозначения показателя* | *Факторы, учитываемые при оценке показателя* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1 | Цена информации i-го источника | $C_{ni}$ | Гриф секретности |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| 2 | Вероятность k-й угрозы информации i-го источника | $P_{yki}$ | $P_{yki} = P^{(пу)}_{yki} \cdot P^{(эу)}_{yki} \cdot P^{(ву)}_{yki}$ |
| 3 | Ущерб от k-й угрозы информации i-го источника | $C_{yki}$ | $C_{yki} = C_{ии} \cdot P_{yki}$ |
| 4 | Затраты на предотвращение k-й угрозы информации i-го источника | $C_{зki}$ | Затраты на проектирование, закупку, установку и эксплуатацию технических средств и реализацию организационных мер |
| 5 | Эффективность меры на предотвращение k-й угрозы информации i-го источника | $W_{зki}$ | $W_{зki} = C_{yki} / C_{зki}$ |

*Примечание.* $P^{(пу)}_{yki}$, $P^{(эу)}_{yki}$, $P^{(ву)}_{yki}$ — вероятности выполнения пространственного, энергетического и временного условий разведывательного контакта.

На цену защищаемой информации влияют собственные затраты организации при ее получении, ожидаемая прибыль от применения информации, ущерб при попадании этой информации к злоумышленнику. В первом приближении цена защищаемой информации пропорциональна грифу ее секретности. Но значения грифа секретности образуют порядковую шкалу. У каждого человека формируется собственное опорное представление о количественной мере качественного значения лингвистической переменной. Например, для одного человека цена одного и того же товара очень малая, для другого — очень большая. Учитывая, что задача оптимизации системы защиты решается в конкретной организации для уменьшения субъективизма, в качестве опорной меры целесообразно использовать экспертную оценку в организации количественной меры базового значения «большая» цена или «большие» расходы.

Попадание к противнику информации, составляющей тайну организации, может нанести ей ущерб, который в общем случае оценивается в зависимости от мощности организации как сред-

ний или большой. Например, если грифу «секретно» можно сопоставить значение (х) цены информации как большая — $x^1$, то «совершенно секретно» — чрезвычайно (очень, очень) большая — $x^2$, «особой важности» — (очень, очень большая)$^2$ — $x^4$.

Еще большая неопределенность возникает при определении значений вероятности угрозы. Единственная возможность повысит достоверность оценки — расчленение этого показателя на составляющие и определение значений этих составляющих, что сделать обычно проще, чем оценить значение интегрального показателя. Для получения информации злоумышленником необходимо выполнить ряд этапов и процессов, которые можно свести к трем условиям разведывательного контакта злоумышленника с источником информации:

— поиск и обнаружение источника информации;
— размещение технического средства добывания на удалении от источника, при котором обеспечивается приемлемое отношение сигнал/шум на входе средства;
— совпадение времени и проявления демаскирующих признаков объекта защиты или передачи семантической информации и работы средства добывания.

Угроза реализуется при одновременном выполнении этих условий, а вероятность ее равна произведению соответствующих вероятностей.

С учетом рассмотренных предложений значения показателей алгоритма проектирования системы защиты информации указаны в табл. 27.12.

*Таблица 27.12*

| *№ п/п* | *Лингвистические переменные* | *Значения показателей* | *Алгебраические выражения для вычисления значений показателей* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| 1 | Цена информации | $x^n y_и$ | |
| 2 | Вероятность выполнения пространственного условия | $x^p y_{пу}$ | |
| 3 | Вероятность выполнения энергетического условия | $x^r y_{эу}$ | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 4 | Вероятность выполнения временного условия | $x^g y_{ву}$ | |
| 5 | Вероятность угрозы | $x^m y_y$ | $x^m y_y = x^{p+r+g}(y_{пу} y_{эу} y_{ву})$ |
| 6 | Ущерб от угрозы | $x^s y_{yy}$ | $x^s y_{yy} = x^{n+m}(y_и y_y)$ |
| 7 | Затраты на меру защиты | $x^l y_э$ | |
| 8 | Эффективность меры по защите | $x^h y_э$ | $x^h y_э = x^{s-j}(y_{yy} / y_э)$ |

*Примечание.* 1. В выражениях табл. 27.12 опущены для упрощения записи индексы i и k обозначения i-го источника и k-й угрозы;
2. $y_{пу} \cdot y_{эу} \cdot y_{ву} \to y_{yy}$; $y_и \cdot y_y \to y_{yy}$; $y_{yy} / y_э т \to y_э$.

**Пример. 1. Исходные данные:**

- цена информации — очень большая ($x^2 y_и$);
- вероятность выполнения пространственного условия — малая ($x^{-1} y_{пу}$);
- вероятность выполнения энергетического условия — малая ($x^{-1} y_{эу}$);
- вероятность выполнения временного условия — средняя ($x^0 y_{ву}$);
- затраты на меру защиты — малые ($x^{-1} y_э$).

**2. Производные показатели:**

- вероятность угрозы — $x^{-1-1+0} y_y = x^{-2} y_y$ — очень малая угроза;
- ущерб от угрозы — $x^{2-2} y_{yy} = x^0 y_{yy}$ — средний;
- эффективность меры защиты — $x^{0+1} y_э$ — высокая.

Для цены информации «большая» при тех же остальных исходных данных:

- ущерб от угрозы — $x^{1-2} y_{yy} = x^{-1} y_{yy}$ — малый;
- эффективность меры защиты — $x^{-1+1} y_э = x^0 y_э$ — средняя.

Таким образом, рассмотренный аппарат позволяет производить простейшие операции непосредственно со значениями лингвистических переменных без промежуточного перевода их в числовые значения. Для одинакового восприятия значений лингвистических переменных разными людьми необходимо базовое значение прокомментировать соответствующим по мнению лица, производящего оптимизацию, числовым значением.

Рассмотренный аппарат может найти применение не только для решения задач защиты информации, но и любых других слабоформализуемых задач, при решении которых применяются качественные шкалы.

### Вопросы для самопроверки

1. Этапы алгоритма проектирования (модернизации) системы защиты информации.
2. Условия завершения оптимизации и функции обратной связи в алгоритме проектирования (модернизации) системы защиты информации.
3. Виды моделей, применяемые при проектировании системы защиты информации.
4. Основные процессы, выполняемые при моделировании объектов защиты.
5. Основные процессы моделирования угроз информации.
6. Типы злоумышленников, проникающих в организацию.
7. Математический аппарат, применяемый для моделирования каналов несанкционированного доступа к информации.
8. Основные процедуры и показатели моделирования каналов утечки информации.
9. Рекомендации по оценке риска утечки информации по оптическому каналу утечки.
10. Рекомендации по оценке риска утечки информации по акустическому каналу.
11. Рекомендации по оценке риска утечки информации по радиоэлектронному каналу.
12. Основные положения математического аппарата, рекомендуемого для оценки показателей моделирования системы инженерно-технической защиты информации.

# Глава 28. Методические рекомендации по определению мер инженерно-технической защиты информации

## 28.1. Общие рекомендации

Так как не существует формальных методов синтеза вариантов предотвращения угроз информации, то разработка мер по защите информации проводится эвристическим путем на основе знаний и опыта соответствующих специалистов. Перечень типовых способов и средств защиты информации приведен в табл. 28.1.

*Таблица 28.1*

| *Угрозы и способы их реализации* | *Типовые способы и средства предотвращения угроз* |
|---|---|
| *1* | *2* |
| Физический контакт злоумышленника с источником информации | Механические преграды (заборы, КПП, двери, взломостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз |
| Пожар | Технические средства пожарной сигнализации, средства пожаротушения, огнестойкие хранилища и сейфы |
| Наблюдение | Маскировочное окрашивание, естественные и искусственные маски, ложные объекты, аэрозоли, пены, радиолокационные отражатели, радио- и звукопоглощающие покрытия, теплоизолирующие материалы, генераторы радио- и гидроакустических помех |
| Подслушивание | Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие материалы, акустическое и вибрационное зашумление, обнаружение, изъятие и разрушение закладных устройств |
| Перехват | Выполнение требований по регламенту и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование, пространственное и линейное зашумление |

| *1* | *2* |
|---|---|
| Утечка информации по вещественному каналу | Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов |

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в табл. 28.2.

*Таблица 28.2*

| *Угроза* | *Способы предотвращения угрозы* | *Средства предотвращения угрозы* | *Затраты на предотвращения угроз* | *Выбранные способы и средства предотвращения угроз* | *Затраты на выбранные способы и средства* |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| ... | ... | ... | ... | ... | ... |
| | | | | | |

Совокупность рассмотренных таблиц, планов и схем с результатами моделирования объектов защиты и угроз, а также предложений по способам и средствам защиты информации создают основу проекта по построению соответствующей системы или предложений по совершенствованию существующей системы.

В итоговой части проекта (служебной записке, предложениях) целесообразно оценить полноту выполнения задач по защите информации для выделенных ресурсов, а также нерешенные задачи и необходимые для их решения ресурсы.

Подготовленные документы (проект, служебная записка, предложения) предъявляются руководству для принятия решения. Наличие в них нескольких вариантов решений способствует более активному участию в построении или совершенствованию системы защиты информации руководителя организации в качестве как наиболее опытного и квалифицированного специалиста, так и распорядителя ресурсов организации.

После принятия проекта (предложений) начинается этап их реализации. Основные задачи специалистов по защите информации

заключаются в контроле за работами по выполнению организационных и технических мероприятий, участие в приемке результатов работ и проверке эффективности функционирования элементов и системы защиты в целом.

Результаты оформляются в виде предложений (проекта) в кратком сжатом виде, а материалы моделирования — в виде приложения с обоснованием предложений.

В заключение следует отметить, что материалы с предложениями и их обоснованием, в которых раскрываются методы и средства защиты информации, нуждаются в обеспечении высокого уровня безопасности, а обобщенные документы должны иметь наиболее высокий гриф из применяемых в организации.

## 28.2. Методические рекомендации по организации физической защиты источников информации

После определения мест размещения источников информации в контролируемых зонах возникает задача определения характеристик этих зон, влияющих на уровень защиты информации в этих зонах. Так как основу физической защиты составляют инженерные конструкции, то в качестве исходных данных для моделей зон используется строительная документация территории и зданий организации, в том числе поэтажные планы зданий. По ней определяются характеристики заборов, зданий, помещений, влияющие на защищенность источников информации от преднамеренных воздействий. Особое внимание обращается на уязвимые места: окна, двери, чердачные, разгрузочные и прочие люки, некапитальные стены, потолки, вентиляционные отверстия, воздуховоды и другие конструкции, которые могут быть открыты, проломлены, разрушены злоумышленником.

Далее работу по организации продолжают сотрудники службы безопасности, решающие рассматриваемую задачу.

Имеющейся после проведенной работы исходных данных достаточно для оценки величины угрозы, в том числе вероятности обнаружения злоумышленника имеющимися средствами обнаружения и видеоконтроля, а также времени преодоления рубежей с использованием носимого инструмента.

В случае недостаточности защищенности источников информации проводится работа по укреплению физической защиты. Она включает:

- выбор (уточнение) зон и рубежей защиты;
- выбор (уточнение) вида охраны — автономной или централизованной;
- определение структуры и значимости рубежей защиты, на которых устанавливаются средства сигнализации — рубежей охраны;
- определение характеристик блокируемых участков рубежей охраны (фасада, тыла, перехода, правой или левой сторон, дверь, окно и др.);
- прогнозирование возможного способа преодоления злоумышленником блокируемого участка рубежа охраны (открывание, пролом, разрушение, их комбинация или иные способы);
- выбор технических средств обнаружения и видеоконтроля.

В качестве зон используются, как правило, типовые архитектурные конструкции организации:

- на территории организации — двор, подсобные и складские помещения, здания;
- внутри здания — коридоры, отсеки в коридорах, переходы между зданиями, помещения, шкафы, сейфы, хранилища.

На границах зон создаются рубежи:

- забор, КПП, ворота основные и запасные;
- периметр открытых площадок во дворе организации;
- основные и запасные двери зданий;
- двери разгрузочных люков;
- двери коридора;
- периметр коридора;
- окна помещений на 1–2-м и последних этажах, возле высоких деревьев и пожарных лестниц;
- стены;
- потолки;
- полы.

Многообразие указанных архитектурно-строительных зон и рубежей позволяет создавать из них на пути возможного движения злоумышленника зоны и рубежи физической защиты, обеспечивающие требуемый уровень безопасности информации.

### 28.2.1. Рекомендации по повышению укрепленности инженерных конструкций

#### *28.2.1.1. Рекомендации по повышению укрепленности ограждения периметра предприятия (организации, учреждения)*

Укрепленность ограждений зависит, прежде всего, от категории объекта защиты. В качестве максимальных требований рекомендуются следующие меры:

1. Высота и вид ограждения периметра должны существенно затруднить его преодоление: высота — не менее 2,5 м с козырьком по верху с ограждением из 3–4 рядов оцинкованной колючей проволоки. Ограждения должны быть по возможности прямолинейными, с минимальным количеством изгибов и поворотов, а также впадин и бугров на поверхности земли.

2. С внутренней стороны ограждения периметра устанавливается зона отторжения шириной не менее 1,5 м и предупредительное ограждение. В зоне отторжения размещаются средства обнаружения и наблюдения, охранное и дежурное освещение, постовые грибки со связью для охраны, разграничительные и указательные знаки. Для обнаружения следов злоумышленников на почве целесообразно создание контрольно-следовой полосы. Предупредительное ограждение высотой не менее 1,5 м из металлической сетки, проволоки, досок (штакетника) затрудняет проникновение на контрольно-следовую полосу сотрудников организации и животных.

#### *28.2.1.2. Рекомендации по повышению укрепленности зданий и помещений*

Так как наиболее слабыми элементами зданий и помещений являются двери и окна, то, прежде всего, повышают прочность дверей и окон. Прочные двери должны соответствовать следующим условиям:

1. Входные деревянные двери должны иметь толщину не менее 40 мм с двумя несамозащелкивающимися врезными замками. Двери, выходящие во двор организации, чердаки и подвалы, а также в местах хранения материальных ценностей и ценных источников информации, должны быть обиты с двух сторон оцинкованной

сталью толщиной не менее 0,6 мм с загибом краев листа на торцы дверного полотна. Стальной лист крепится по периметру и диагонали с шагом не более 50 мм гвоздями диаметром 3 мм и длиной 40 мм. Дверная коробка зданий и помещений выполняется из стального профиля или дерева, усиленного стальными уголками размером 30 × 40 × 5 мм. Уголки крепятся к стене с помощью стальных костылей диаметром не менее 10 мм и длиной не менее 120 мм.

2. Двери люков изнутри запираются на запоры, а снаружи — на навесные замки. Деревянная обвязка люков крепится к фундаменту стальными скобами или костылями диаметром не менее 16 мм и длиной не менее 150 мм.

3. Помещения, в которых размещаются материальные ценности, в том числе и источники ценной информации, могут оборудоваться с внутренней стороны дополнительными решетчатыми раздвижными или распашными дверями с ушками для навесного замка.

4. Оконные проемы на первых этажах, вблизи пожарных лестниц, над козырьками заборов и примыкающими строениями оборудуются стационарными или съемными раздвижными (распашными) решетками или ставнями. Ставни изготовляются из досок или фанеры толщиной не менее 12 мм, обитых листовой сталью. Они запираются на задвижки и навесные замки. Витринные проемы зданий защищаются стационарными или раздвижными (распашными) решетками. Решетки выполняются из стального прутка диаметром не менее 16 мм с ячейками 150 × 150 мм. Раздвижные и съемные решетки могут изготавливаться из стальной полосы сечением не менее 4 × 30 мм с ячейками не более 180 × 180 мм. В местах пересечений прутья и полосы свариваются.

5. Теплопроводы, дымоходы, вентиляционные шахты и вентиляционные короба размером более 200 × 200 мм, имеющие выход на крышу или в другие помещения, защищаются глухими решетками. Решетка в вентиляционных коробах со стороны помещения может отстоять от стены или перекрытия на расстояние не более 100 мм.

### 28.2.2. Выбор технических средств охраны

Многообразие технических средств физической защиты порождает весьма сложную задачу их рационального выбора для конкретных условий по критерию эффективность-стоимость. На

рубежах охраны технические средства обнаружения определяются с учетом вида рубежа, способов обнаружения злоумышленника и пожара, а также значений конкретных тактико-технических характеристик (ТТХ) средств охраны.

### *28.2.2.1.Выбор извещателей*

Тип извещателя выбирается с учетом вида охраняемого рубежа или зоны, их размеров и конфигурации, вида воздействия злоумышленника и помех на преграду, затрат на приобретение, установку (строительство) и эксплуатацию инженерных конструкций и технических средств.

Эффективное использование технических возможностей извещателей достигается, когда размеры блокируемого участка (зоны) близки к соответствующим характеристикам извещателя. Рекомендуемое соотношение между длиной (площадью) $L_{бл}(S_{бл})$ реальной охраняемой (блокируемой) зоны и максимальной дальностью (площадью) зоны охраны $L_{из}(S_{из})$ извещателя: $L_{бл}(S_{бл}) = (0,7– 0,9)L_{из}(S_{из})$.

Виды воздействий злоумышленников на механические преграды указаны в табл. 28.3.

*Таблица 28.3*

| *№ п/п* | *Объект охраны* | *Вид воздействия* |
|---|---|---|
| 1 | Капитальные стены | Удар, разрушение |
| 2 | Некапитальные стены и перегородки | Пролом |
| 3 | Металлические двери и ворота | Открывание, удар |
| 4 | Дверные проемы, погрузочно-разгрузочные люки, деревянные ворота | Открывание, пролом |
| 5 | Остекленные конструкции | Открывание, разрушение |
| 6 | Вентиляционные короба | Открывание, разрушение |

Существенное влияние на выбор извещателя оказывает помеховая ситуация в районе его размещения в интервале времени, когда он находится во включенном состоянии. Помеховая ситуация может существенно изменяться. Например, рядом с охраняемым

зданием могут начаться строительные работы с использованием тяжелой техники, работа которой вызывает значительные акустические помехи. Усредненное влияние помех различных типов на извещатели характеризуется данными табл. 28.4.

*Таблица 28.4*

| № п/п | Вид помехи | Вид извещателя | | | | |
|---|---|---|---|---|---|---|
| | | акустический | оптико-электронный | радиоволновый | емкостной | вибрационный |
| 1 | Внешние акустические шумы (уличные, раскаты грома и др.) | + | – | – | – | + |
| 2 | Внутренние (в контролируемой зоне) акустические шумы (холодильники, ТА, шум воды в трубах и др.) | + | – | – | – | – |
| 3 | Внешний свет (свет фар, солнечные блики) | – | + | – | – | – |
| 4 | Движение воздуха в помещении (сквозняки, вентиляторы, батареи отопления) | – | + | – | – | – |
| 5 | Движение предметов (штор, лопастей вентилятора, воды на стеклах, листьев и др.) | + | + | + | – | – |
| 6 | Электромагнитные помехи (сварочные ап-ты, разряды высоковольтных линий, трамваев, троллейбусов, люминесцентные лампы и др.) | – | – | – | + | – |
| 7 | Мелкие животные, крупные насекомые | + | + | + | + | + |

*Примечание.* Знак + указывает на сильное влияние помехи на работу извещателя, знак – указывает на отсутствие такого влияния.

### *28.2.2.2. Выбор шлейфов*

Количество шлейфов на каждом рубеже охраны определяется его конфигурацией и протяженностью. Чем на большее количест-

во участков разделяется рубеж охраны, тем с большей точностью определяется местонахождение злоумышленника и тем эффективнее можно организовать его нейтрализацию. Но при этом для большинства применяемых извещателей пропорционально возрастает число шлейфов. Для охраны периметра организации и зданий рекомендуются следующие участки: фасад, тыл, правая и левая стороны с контролем каждого участка отдельным извещателем со шлейфом. Отдельными шлейфами могут быть соединены извещатели, установленные в охраняемых зонах (переходах, коридорах) на объектах охраны сложной конфигурации.

Так как пожарная сигнализация в отличие от охранной работает в круглосуточном режиме, то рекомендуются раздельная и раздельно-совмещенные разновидности структуры охранной сигнализации на рубеже защиты. В раздельной структуре автономные пожарные и охранные шлейфы подключены не только к разным контрольно-приемным пунктам (ПКП) автономной системы охраны, но и к разным номерам пультов централизованного наблюдения (ПЦН) централизованной системы охраны. В раздельно-совмещенной системе пожарные и охранные шлейфы подсоединены в автономной системе к своим ПКП, а в централизованной — к единому номеру ПЦН. В совмещенной разновидности структуры, в которой охранные и пожарные извещатели подсоединены к одному шлейфу, обнаружение пожара возможно лишь в то время, когда объект находится под охраной — во внерабочее время.

Квалифицированный злоумышленник в общих чертах представляет современную организацию инженерной защиты и то, что на типовых рубежах защиты (заборе, стенах, дверях, окнах) устанавливаются извещатели. Поэтому для повышения эффективности применяют так называемые **ловушки**, представляющие собой небольшие дополнительные скрытные зоны охраны на возможном пути движения злоумышленника, о которых не должен догадываться злоумышленник. Ловушками оборудуются локальные участки (тамбуры между дверьми, коридоры и другие участки), ведущие в помещения с объектами охраны. Для обеспечения ловушек применяют в основном магнито-контактные и оптико-электронные извещатели.

### *28.2.2.3. Выбор средств наблюдения и мест их установки*

Учитывая сравнительно высокую стоимость телевизионных камер и их эксплуатации, в том числе необходимость постоянного наблюдения изображения от них на экранах мониторов, камеры устанавливают в местах с максимальной потенциальной угрозой.

К таким местам относятся:

- входы в офис, организацию, на контрольно-пропускной пункт;
- территория организация со слабой защитой (двор со складированной продукцией, стоянка служебного автотранспорта возле организации и др.);
- в операционные залы и боксы для остановки инкассаторских машин;
- подступы к выделенным помещениям (в коридорах);
- места хранения ценных объектов защиты (помещениях, хранилищах, возле сейфов).

Телевизионная камера выбирается с учетом:

- категории значимости объекта;
- геометрических размеров зоны охраны;
- информативных демаскирующих признаков объектов наблюдения;
- освещенности зоны охраны в разное время суток;
- расположения возможных мест проникновения злоумышленника в охраняемую зону;
- условий эксплуатации;
- вида наблюдения — скрытого или открытого.

Влияние категории объекта проявляется в более высоких требованиях к качеству телевизионной камеры, прежде всего, к разрешающей способности и чувствительности. Для объектов категории А рекомендуется применять не только высококачественные черно-белые, но и цветные телевизионные камеры.

Наибольшая неопределенность возникает при выборе фокусного расстояния объектива. Выбор зависит от необходимого угла зрения объектива, геометрических размеров охраняемой зоны, требуемого для идентификации объектов наблюдения разрешения камеры. Чем больше угол зрения объектива, тем меньше масштаб изображения и ниже возможность идентификации объектов наблюдения. Для увеличения масштаба изображения на экране монитора необходим объектив с большим фокусным расстоянием, но у него

меньший угол и глубина зрения. Учитывая противоречивую зависимость факторов, влияющих на выбор объектива, следует в качестве исходных данных использовать следующие требования к качеству изображения на экране монитора:

- соответствие поля изображения зоне охраны;
- обеспечение требуемого уровня детализации признаков объекта наблюдения.

Выполнение первого требования обеспечивается при горизонтальном угле зрения $\alpha_г$ камеры, определяемом исходя из размеров и конфигурации зоны охраны, а также рекомендаций и ограничений по ее установке. При выборе места установки камеры целесообразно:

- по возможности исключить засветку объектива камеры прямым или отраженным солнечным светом или искусственным светом;
- в поле зрения должны попасть места (окна, двери, люки и т. п.), через которые возможно проникновение злоумышленника;
- размеры непросматриваемой («мертвой») зоны не должны позволить злоумышленнику проникнуть в охраняемую зону и (или) преодолеть рубеж не замеченным.

Кроме того, для исключения засветки изображения рекомендуется:

- не ориентировать камеру в южную сторону, против прямых солнечных лучей и не направлять ее на блестящие, хорошо отражающие свет предметы (зеркала, лужи, стекло окон и др.);
- при установке на открытой местности для защиты от прямых солнечных лучей применять кожухи с козырьком и фильтром;
- устанавливать камеру в верхней части помещения (на потолке, в верхней части стены или угла) с наклоном объектива вниз.

Для примера на рис. 28.1 приведен вариант установки камеры в углу помещения.

Для указанной конфигурации требуемый угол зрения камеры $\alpha_г$ определяется из простых геометрических построений: $tg\alpha_г \approx H / L$, где L — расстояние от объектива камеры границы зоны охраны, H — ширина зоны охраны (помещения).

Для охраны помещений и открытых пространств применяются телевизионные камеры с углом зрения 60–90° или менее широкополосные, устанавливаемые на поворотных платформах. Для ох-

раны периметров применяются узкополосные камеры, устанавливаемые вдоль периметра.

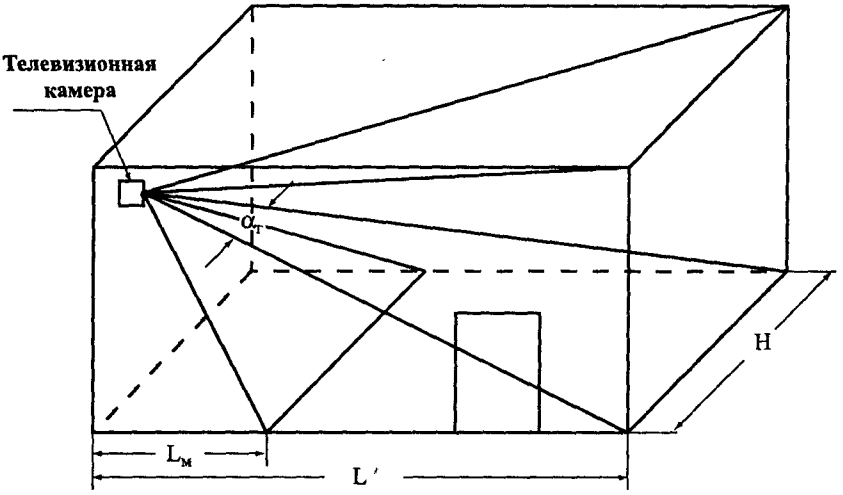



*Рис. 28.1.* Схема установки телевизионной камеры в помещении

Чем больше угол зрения объектива камеры, тем больше размеры наблюдаемой зоны, но тем хуже разрешение изображения наблюдаемого объекта. Между углом зрения объектива и его фокусным расстоянием f существует однозначная зависимость: $\alpha = 2\text{arctg}(h / 2f)$, где h — размер ПЗС-матрицы по горизонтали в мм. В табл. 28.5 указаны количественные значения, соответствующие этой зависимости.

Максимальный угол зрения в 98° имеет объектив с f = 2,8 мм, установленный перед матрицей размером 1/3 дюйма, минимальный — 2,1° у объектива с f = 350 мм и матрицей размером в 1 дюйм.

Для обеспечения требуемого уровня детализации признаков необходимо, чтобы на изображении размеры видовых демаскирующих признаков, используемых для идентификации: государственный номер и тип машины, черты лица злоумышленника, вид оружия у него и др. были не менее минимально допустимых.

*Таблица 28.5*

| *Фокусное расстояние, мм* | *Угол зрения камеры в градусах для размеров матрицы по диагонали в дюймах* | | | |
|---|---|---|---|---|
| | *1/3* | *1/2* | *2/3* | *1* |
| 2,8 | 98 | | | |
| 4 | 64 | 86 | | |
| 6 | 42 | 58 | | |
| 8 | 33 | 42 | 55 | |
| 12 | 22 | 30 | | |
| 16 | 17 | 23 | 30 | 43 |
| 25 | 11 | 14 | 19 | 28 |
| 50 | 5,5 | 7 | 10 | 15 |
| 75 | 3,6 | 5 | 6,6 | 10 |
| 100 | | | 5 | |
| 150 | | | | 4,9 |
| 235 | | | | 3,1 |
| 450 | | | | 2,1 |

Угол зрения $\alpha_p$, требуемый для различения на объекте наблюдения его деталей с минимальными размерами, можно оценить по формуле: $\alpha_p = 2\text{arctg}(sR / 150L)$, где s — минимальный размер в мм детали объекта наблюдения; L — расстояние от камеры до наблюдаемого объекта в м; R — разрешение камеры в ТВЛ.

Величина фокусного расстояния объектива для обеспечения наблюдаемости деталей изображения оценивается по формуле: $f_p = 75Lh / sR$.

Фокусные расстояния объективов, выбранные исходя из геометрических размеров зоны охраны и обеспечения необходимого разрешения объекта наблюдения, как правило, не совпадают. Возможны следующие пути решения этого несоответствия:

- для увеличения зоны наблюдения применяют поворачивающие платформы камер;
- для повышения разрешения камеры используются объективы с переменным фокусным расстоянием — вариообъективы.

Второй путь предпочтительней, так как при наблюдении оператором (охранником) всей зоны охраны вероятность обнаружения злоумышленника выше, чем при наблюдении ее отдельных участ-

ков. При применении вариообъективов телевизионная камера работает в двух режимах: обзорного и детального наблюдения. В режиме обзорного наблюдения фокусное расстояние устанавливается с учетом видимости всей зоны охраны. При появлении в поле зрения камеры злоумышленника или подозрительного объекта фокусное расстояние увеличивают до обеспечения требуемого разрешения деталей на объекте наблюдения. При выборе камеры по чувствительности учитывается минимальная освещенность объекта и диапазон ее изменения. Различают освещенность объекта $E_{об}$ и освещенность ПЗС-матрицы $E_{матр}$. Эти величины связаны между собой выражением:

$$E_{матр} = E_{об}\alpha_{отр} / \pi f^2,$$

где $\alpha_{отр}$ — коэффициент отражения объекта.

Для реальных объектов освещенность объекта может превышать освещенность на матрице в 10 раз. Некоторые значения коэффициента отражения указаны в табл. 28.6.

*Таблица 28.6*

| *Объект* | *Коэффициент отражения* |
|---|---|
| Пустой чистый асфальт | 0,05—0,1 |
| Трава, кусты, деревья | 0,2—0,25 |
| Красный кирпич | 0,35—0,4 |
| Автомобиль | 0,4—0,5 |
| Стекло | 0,7—0,8 |
| Белая краска | 0,55—0,75 |
| Снежный покров | 0,65—0,85 |

Диапазон изменения освещенности в помещениях существенно меньше диапазона освещенности открытой местности. В помещении применяются телевизионные камеры с электронным затвором, обеспечивающим 200-кратное изменение выдержки (от 1/50 до 1/10000). Камеры для наружного освещения должны иметь устройства, компенсирующее (1000–2000)-кратное изменение яркости. В качестве таких устройств применяют кроме электронного затвора автодиафрагму.

Яркость и места установки источников дежурного освещения выбираются с учетом следующих требований:

- обеспечение необходимой для обнаружения и распознавания злоумышленника освещенности контролируемых зон и рубежей в ночное время и в неблагоприятных для наблюдения климатических условиях;
- скрытие мест нахождения сил и средств нейтрализации угроз;
- формирование у злоумышленника чувства неуверенности и большого риска в случае проникновения злоумышленника в контролируемую зону и попытки преодоления рубежа;
- минимизация затрат на электроэнергию для источников освещения.

Освещенность пространства, примыкающего к периметру организации, должна быть не менее 1 лк, внутри ограждения — не менее 3 лк, а стены зданий и пешеходных дорожек — не менее 5 лк. Освещение внутри помещений охраны, через окна которого ведется наблюдение, должно быть слабое. В противном случае помещение будет хорошо просматриваться, а наблюдение из него затруднено. Кроме того, при выходе охранника из помещения с ярким освещением в темное место его зренню для адаптации потребуется несколько минут, в течение которых у злоумышленника появляется возможность произвести нападение, спрятаться или убежать. Окна этого помещения целесообразно закрыть сетчатыми занавесками, а внутренние поверхности оконных рам окрасить в черный цвет.

## 28.3. Рекомендации по предотвращению утечки информации

### 28.3.1. Типовые меры по защите информации от наблюдения:

**а) через окна:**

- уменьшение освещенности объектов в помещении;
- уменьшение прозрачности окон путем применения:
  - — занавесок;
  - — штор;
  - — жалюзи;
  - — тонированных стекол и пленок на окнах.

Следует отметить, что применение тонированных стекол или пленок создает дополнительные демаскирующие признаки для определения извне места нахождения выделенного помещения. Поэтому для скрытия этого признака целесообразно применить такие стекла или пленки на других окнах, хотя бы соответствующего этажа.

**б) через приоткрытую дверь:**

- применение доводчика двери;
- установка на дверь замка (лучше кодового) с защелкой.

**в) на экране компьютера:**

- ориентация экранов мониторов на рабочих местах сотрудников, исключающих наблюдение изображений на них через открытую дверь;
- установка минимального (1–2 минуты) интервала включения заставки на экране монитора для исключения отображения информации в перерывах работы.

**г) на открытых площадках:**

- применение искусственных масок;
- маскировочное окрашивание;
- засветка и ослепление наблюдателя с помощью ярких источников света, лучи которого направлены в сторону наблюдателя и попадают на изображение объекта наблюдения (засветка) и на поле изображения (ослепление);
- покрытие объекта пеной;
- использование дымов;
- создание ложных объектов прикрытия.

**д) с помощью РЛС БО, устанавливаемых на самолетах и космических аппаратах:**

- применение искусственных масок, изменяющих направление отражения электромагнитных волн или их поглощение;
- размещение на сложном объекте радиоотражающих средств, искажающих его достоверное изображение;
- размещение в пространстве фона радиоотражающих средств, деформирующих изображение фона;
- излучение помех, имитирующих ложные объекты.

### 28.3.2. Типовые меры по защите информации от подслушивания:

**а) через дверь:**

- устранение щелей между дверным полотном и дверной рамой;
- повышение поверхностной массы дверного полотна;
- покрытие дверного полотна звукопоглощающими материалами;
- установка второй двери с тамбуром.

**б) через приоткрытую дверь:**

- установка на дверь доводчика;
- установка на дверь замка с защелкой.

**в) через окна:**

- закрытие окон;
- установка звукоизолирующих прокладок между оконными рамами;
- закрытие окна плотными шторами;
- виброакустическое зашумление стекол окон;
- тройное остекление.

**г) через стены:**

- увеличение толщины и поверхностной массы стены путем дополнительной кирпичной кладки и установки экранов;
- покрытие стены звукопоглощающими материалами;
- виброакустическое зашумление.

**д) через вентиляционные отверстия:**

- установка перед вентиляционными отверстиями экранов;
- установка в вентиляционные отверстия глушителей.

**е) через водоотопительные системы:**

- установка перед батареями отопления и труб акустических экранов;
- установка в вентиляционные отверстия глушителей.

**ж) через функциональные каналы связи:**

- соблюдение дисциплины связи;
- техническое закрытие электро- и радиосигналов;
- шифрование сообщений.

**з) через ПЭМИН:**

- выключение неиспользуемых радиосредств и электрических приборов;
- включение между защищаемым средством и линией устройства фильтрация и уменьшения малых амплитуд побочных опасных сигналов;
- применение буферов между РЭС и информационными кабелями;
- экранирование радиоизлучающих ОТСС;
- экранирование кабелей и проводов;
- симметрирование кабелей;
- линейное и пространственное зашумление.

**и) через закладные устройства:**

- поиск закладных устройств с помощью средств обнаружения их радио- и электрических сигиалов, полупроводниковых и металлических элементов закладных устройств, просвечивания возможных мест их размещения средствами интроскопии;
- использование средств обнаружения работающего диктофона и подавление его сигналов;
- подключение к линиям связи и цепям электропитания средств, создающих сигналы, изменяющих режимы работы закладных устройств или разрушающих их входные цепи;
- зашумление среды распространения сигналов закладных устройств.

### 28.3.3. Типовые меры по защите информации от перехвата:

**а) побочных электрических сигналов:**

- фильтрация опасных сигналов;
- линейное зашумление.

**б) побочных радиосигналов:**

- экранирование помещений и ограждений на отдельных направлениях;
- экранирование проводов входящих (выходящих) кабелей;
- симметрирование кабелей и полей;
- зашумление помещений.

**в) сигналов функциональных каналов связи:**

- соблюдение дисциплины связи;

- техническое закрытие;
- шифрование сообщений.

### 28.3.4. Методические рекомендации по «чистке» помещений от закладных устройств

Поиск закладных устройств в помещениях («чистка» помещений) можно рассматривать как контрразведывательную операцию, эффективность которой зависит от ее методического обеспечения. Методические рекомендации по «чистке» помещений рассмотрены в [2, 6]. Типовое поисковое мероприятие состоит из трех последовательно выполняемых этапов:

- подготовительного;
- этапа проведения поискового мероприятия;
- заключительного.

Подготовительный этап предусматривает:

- прогноз вероятного противника (злоумышленника, органа разведки) и анализ его оперативно-технических возможностей;
- изучение расположения помещения и его окружения, в котором могут находиться источники угроз, в том числе конструктивных особенностей здания и его ограждений;
- определение находящихся в помещении мебели, предметов интерьера, радиосредств, электрических приборов и других устройств, которые могут быть использованы для размещения закладных устройств;
- изучение планов обследуемых и смежных помещений и схем коммуникаций;
- изучение режима посещения помещения сотрудниками организациями и посетителями других организаций;
- установка фактов ремонта, монтажа или демонтажа коммуникаций, замены мебели и других работ, выполняемых посторонними лицами;
- определение (уточнение) методики поискового мероприятия для конкретного помещения;
- определение перечня поисковой аппаратуры;
- разработка легенды и вариантов поведения, обеспечивающих оперативное прикрытие работы поисковой бригады;
- разработка плана активизации злоумышленника и закладных устройств;

- предварительный осмотр обследуемого и смежных помещений;
- разработка плана проведения поисковых мероприятий.

Так как определение возможных злоумышленников — одна из задач службы безопасности организации, то у руководителя службы организации к моменту проведения поисковых мероприятий должны быть факты и соображения по вероятному противнику организации. В результате совместного прогноза руководителей службы безопасности и поисковой бригады ранжируется перечень источников угроз: спецслужба, конкурент или криминал. Целесообразно привлечь к этой работе руководителя организации. Эти прогнозы важны для разработки замысла поиска и состава поисковых средств. Например, для внедрения дистанционно управляемых закладных устройств необходимы несколько технически подготовленных людей с возможностью их конспиративного захода в помещение на короткое время, что по силам в основном спецслужбам. Прогноз злоумышленника позволяет также создать модель используемого им технического средства добывания информации. На основании такой модели формулируются требования к поисковому средству, обеспечивающему обнаружение закладного устройства.

Важнейшей задачей, решаемой на предварительном этапе, является создание условий для скрытности работы поисковой бригады. Конспиративный поиск позволяет:

- локализовать место нахождения приемника сигнала канала утечки и через него выйти на установщика закладного устройства и «заказчика»;
- исключить противодействия злоумышленника поисковым мероприятиям.

Утечка информации о проверке может свести на нет дорогостоящее поисковое мероприятие, если злоумышленнику удастся изъять закладное устройство на время работы поисковой бригады.

Для обеспечения скрытности поиска разрабатывается легенда появления поисковой бригады в организации и ее работы, а также определяются варианты поведения поисковиков на территории организации вне обследуемого помещения. Поведение и разговоры членов поисковой бригады должны соответствовать легенде. Например, если во время обеда в столовой или месте, отведенном для курения, члены поисковой бригады будут обсуждать ход поиска, то могут быть раскрыты их истинные задачи. Чтобы не вызвать

подозрение у злоумышленника, легенда прикрытия должна правдоподобно объяснять работу поисковой бригады на всех этапах работы не только в обследуемом помещении, но и других местах, где проводятся проверки. Не исключено, что злоумышленник может попытаться установить контакт с членами бригады для выяснения истинных причин их появления в организации.

Учитывая, что состав поисковой аппаратуры зависит от вида обследуемых объектов, она разделяется на 4 группы:

- для проверки электронных устройств;
- для проверки мебели и предметов интерьера;
- для проверки электроустановочных изделий;
- для проверки ограждений.

На подготовительном этапе разрабатывается документы, основными из которых являются следующие:

- перечень лиц, допущенных к поисковым мероприятиям;
- планы прилегающей местности с радиусом до 1 км с указанием мест возможного размещения приемников сигналов закладных устройств;
- поэтажные планы здания, в котором находится обследуемое помещение с указанием характеристик этих и смежных помещений;
- план-схема коммуникаций организации с указанием щитов и разводных коробок;
- план обследуемого помещения с указанием размещенных в нем предметов, средств и приборов, в которых могут быть установлены или к которым могут быть подключены закладные устройства;
- характеристики прогнозируемых закладных устройств и приемников их сигналов;
- легенды прикрытия поисковых мероприятий;
- перечень поисковой аппаратуры разных групп;
- план работы поисковой бригады с указанием сроков и исполнителей.

Поисковые мероприятия начинаются с изучения оперативной обстановки вокруг и внутри организации, которая предусматривает:

- определение и оперативную разработку пунктов приема сигналов закладных устройств;

- фиксирование и скрытное наблюдение за подозрительными автомобилями с пассажирами, время приезда и отъезда которых совпадает с временем пребывания сотрудника, работающего в проверяемом помещении;
- контроль радиоэфира.

Пункт контроля радиоэфира разворачивается в течение поискового мероприятия в нескольких местах здания, в том числе в обследуемом помещении. Контроль радиоэфира завершается через несколько дней после окончания видимой сотрудникам части поискового мероприятия. Это позволяет выявлять не обнаруженные дистанционно управляемые закладные устройства, не включаемые злоумышленником в случае возникновения у него подозрений по поводу задач поисковой бригады. На пункте контроля решаются следующие задачи:

- разработка карты загрузки эфира в районе нахождения помещения;
- выявление и исключение из последующего анализа легальных источников радиоизлучений;
- статистический анализ работы подозрительных источников радиоизлучений.

После перемещения пункта контроля в другое место обращают внимание на сигналы с изменяющейся амплитудой. Заметное изменение амплитуды является признаком нахождения источника радиоизлучения в ближней зоне, т. е. вблизи места нахождения приемника пункта контроля радиоэфира.

Поисковые мероприятия в помещении начинаются с его **визуального осмотра**. Перед осмотром выносятся в другое помещение для проведения специальных исследований все мобильные радиоэлектронные средства. Затем тщательно осматриваются по или против часовой стрелки и от периферии к центру все места, в которых могут быть размещены закладные устройства: щели в плинтусах, полости за картинами, батареями отопления, на шкафах и за шкафами, за карнизами и других местах. Мебель отодвигается, вынимаются и осматриваются ящики письменных столов и их внутренние полости. Вскрываются в выключенном состоянии электрические розетки и выключатели, разбирается электроустановочная арматура, просматриваются стояки и вводы коммуникаций в помещении и возле него.

**Проверка предметов интерьера и мебели** также начинается с визуального осмотра, а затем с использованием поисковых приборов: металлодетекторов, нелинейных локаторов и средств интроскопии. С целью снижения влияния помех аппаратное обследование предметов интерьера и мебели производится с разных направлений при минимальной чувствительности приборов. Деревянные предметы интерьера и мебели чаще проверяются металлодетекторами, содержащие металлические конструкции — нелинейными локаторами, отдельные предметы, не подлежащие разборке, — средствами интроскопии (флюороскопами и рентгенотелевизионными установками). Для распознавания полупроводниковой нелинейности закладных устройств рекомендуется постукивание предмета, обследуемого нелинейным локатором. Отклик на 2-й и 3-й гармониках, возникающий из-за ложной нелинейности, характеризуется неустойчивостью параметров, коррелированной с ударами по предмету.

После проверки на места предметов интерьера и мебели, в которые могут быть установлены закладные устройства, наносятся невидимые в обычном свете, но видимые, например, в ультрафиолетовом свете, метки, которые позволяют во время следующей проверки обнаруживать внедрения.

**Специальные исследования радиоэлектронных средств** предусматривают допустимую по условиям эксплуатации разборку и анализ частей с целью выявления признаков внедрения закладных устройств. Такими признаками являются:

- следы внезаводского вмешательства в электрическую схему после ее изготовления (следы пайки, изменение цвета лакового покрытия в местах подпайки и др.);
- отличия в топологии реальной схемы средства от указанной в документации или в других образцах — эталонах;
- подозрительные излучения сигналов, характеристики которого не соответствуют работе исследуемого средства.

Подозрительные (впаянные вне заводских условий, не соответствующие образцу и др.) элементы схемы подвергаются рентгеноскопии (просвечиванию) с целью определения их конструкции и назначения.

Сравнение исследуемого образца с эталоном — эффективный метод выявления признаков внедрения закладных устройств в ра-

диоэлектронное средство при условии наличия достоверного эталона. Достоверным эталоном является техническая документация завода-изготовителя, но ее получение от иностранных поставщиков проблематично. В качестве эталонов могут использоваться однотипные средства, полученные по иным каналам, чем исследуемое средство, например купленные от разных, независимых друг от друга продавцов.

Если подозрительные излучения создаются закладным устройством в виде радиомикрофона, то оно идентифицируется путем облучения средства акустическим сигналом громкоговорителя, подключенного к звуковому генератору. Наблюдая принятый радиосигнал на экране спектроанализатора или осциллографа, определяют связь его формы и амплитуды с характеристиками акустического сигнала. Следует также учитывать, что подозрительные излучения могут представлять собой побочные высокочастотные излучения, возникающие, например, в результате паразитной генерации дискретных элементов. Независимо от дальнейших результатов специальных исследований радиоэлектронного средства оно должно быть удалено из выделенного помещения, так как является потенциальным источником сигналов радиоэлектронного канала утечки информации.

**Проверка коммуникаций** начинается с прослеживания с использованием схем электропитания и других коммуникаций трасс силовой (электропитания) и слаботочной (трансляционной сети, шлейфов, селекторной связи, телевизионных кабелей и др.) проводки и определения разводных коробок.

Вытягиваются и визуально осматриваются подводящие провода в местах установки коммуникационных изделий, тщательно рассматриваются электрические установочные изделия (розетки, выключатели, осветительные приборы). В случае обнаружения следов вмешательства они снимаются и просвечиваются с помощью рентгеновской установки. Линии проводки исследуются в режиме короткого замыкания и холостого хода. Закорачивая провода линии в местах установки коммутационных изделий, определяют с помощью вольтомметра (тестера) со стороны разводных коробок их принадлежность. После этого измеряют сопротивление линии после размыкания проводов (в режиме холостого хода). Если

к ним ничего не подсоединено и изоляция соответствует требованиям, то сопротивление превышает единицы МОм. Более низкое сопротивление возникает в случае подсоединения к проводам закладных устройств или ухудшения электрической изоляции. В этом случае необходимо обследовать трассу с помощью нелинейного локатора на предмет выявления подключенных к электропроводке полупроводниковых радиоэлектронных средств. Но даже в случае отсутствия признаков закладного устройства целесообразно обратить внимание должностных лиц организации на ухудшение изоляции электрической проводки и необходимость ее замены во избежание в ближайшем будущем короткого замыкания в цепях электропитания, которое может привести к пожару.

**Телефонные линии** обычно проверяют до коробки ввода магистрального телефонного кабеля в здание. Линия под нагрузкой (без отключения), по которой имитируется телефонный разговор, обследуется индикатором поля, с которым перемещается сотрудник поисковой бригады вдоль трассы прокладки телефонной линии. В случае обнаружения подозрительного излучения (с повышенной по сравнению с фоном мощностью) принадлежность этого излучения к закладному устройству определяется путем многократного соединения и рассоединения линии. При наличии закладного устройства характер изменения подозрительного сигнала соответствует характеру связи.

По окончании проверки коммуникаций установочные изделия маркируются, составляется или уточняется схема коммуникаций, а коробки, щиты и телефонные аппараты опечатываются сотрудником службы безопасности организации.

**Проверка ограждений** проводится с помощью нелинейного локатора и рентгеновской установки. Перед проверкой необходимо:

- убрать в смежных помещениях радиоэлектронные средства, которые могут в случае проникновения электромагнитной волны локатора через стены создать ложные сигналы;
- откалибровать средство (определить и установить минимально допустимую мощность излучения).

Для калибровки локатора на обратной стороне вплотную к стене крепится закладное устройство, соответствующее модели про-

гнозируемого средства добывания злоумышленника, и устанавливаются минимальные уровни сигналов, при которых модель еще обнаруживается. Затем в соответствии с инструкцией по применению локатора обследуется ограждение (стена). Местонахождение полупроводниковой или ложной нелинейности локализуется с большей точностью путем снижения мощности нелинейного локатора и помечается клейкой лентой. Предварительное распознавание закладного устройства производится по виду и характеру изменения сигнала отклика. Достаточно информативными признаками ложных сигналов отклика являются:

- нестационарность сигнала при простукивании подозрительного места;
- резкое изменение уровня сигнала при облучении участка стены с двух противоположных направлений — из обследуемого и смежного помещений;
- резкое уменьшение уровня сигнала в результате «выжигания» ложного полупроводника при облучении подозрительного места импульсным локатором с мощностью около 300 Вт;
- периодичность изменения амплитуды сигнала отклика вблизи водяных коммуникаций в стене, вызванных пульсациями потоков воды в трубе при работе водяных насосов.

Достоверное окончательное решение о принадлежности сигнала отклика закладному устройству можно принять в результате вскрытия подозрительного места или просвечивания его рентгеновскими лучами. При выборе рентгеновского аппарата следует иметь в виду, что для просвечивания каждого 1 см бетона необходимо увеличить напряжение на рентгеновской трубке приблизительно на 10 кВ.

При «чистке» помещения следует иметь в виду также то обстоятельство, что закладные устройства в виде электронных стетоскопов могут быть установлены на строительных конструкциях (металлических балках и трубах) за пределами обследуемого помещения, хорошо проводящих на десятки метров звук. В процессе поиска таких закладных устройств обращается внимание на такие элементы конструкции, проходящие через обследуемое помещение и возможные места установки на них стетоскопов.

На заключительном этапе поисковых мероприятий готовятся отчетные документы со схемами и описанием мест срабатывания аппаратуры, вскрытий участков стен, предметов мебели и интерьера, аппаратуры. Отчет завершается оценкой состояния защищенности информации и рекомендациями по его усилению.

### 28.3.5. Меры по защите информации от утечки по вещественному каналу:

**а) семантической информации и видовых признаков:**

- сбор и учет отходов производства;
- уничтожение отходов производства;
- физическое глубокое стирание дисков и дискет.

**б) демаскирующих веществ:**

- возвращение отходов химического производства в производственный процесс;
- очистка отходов, содержащих демаскирующие вещества, путем фильтрации, нагревания, охлаждения и химических реакций;
- захоронение демаскирующих веществ.

### Вопросы для самопроверки

1. Типовые способы и средства предотвращения угроз.
2. Основные процедуры физической защиты источников информации.
3. Рекомендации по повышению укрепленности ограждений.
4. Рекомендации по выбору извещателей и шлейфов.
5. Рекомендации по выбору телевизионной камеры и места ее установки.
6. Типовые меры по защите информации от наблюдения.
7. Типовые меры по защите информации от подслушивания.
8. Основные этапы и средства «чистки» помещений от закладных устройств
9. Типовые меры по защите информации от перехвата ее носителей.
10. Типовые меры по предотвращению утечки информации по вещественному каналу.

## Основные положения раздела V

1. Основу методологии инженерно-технической защиты информации составляет вербальное и математическое моделирование объектов защиты, угроз информации и методические рекомендации по выбору рациональных вариантов инженерно-технической защиты информации. Вербальная модель описывает объект на профессиональном (информационной безопасности) языке. Математическое моделирование предусматривает исследование математических аналогов реальных объектов и процессов. Проектирование системы инженерно-технической защиты информации с требуемыми характеристиками обеспечивается путем поэтапного моделирования объектов защиты, моделирования угроз информации и рационального выбора мер инженерно-технической защиты в соответствии с алгоритмом проектирования (совершенствования) системы защиты.

На этапе моделирования объектов защиты производится определение на основе структурирования перечня сведений, составляющих государственную (коммерческую) тайну, источников защищаемой информации и ее цены, выявление и описание факторов, влияющих на защищенность этих источников. В результате моделирования объектов защиты определяются исходные данные, необходимые для моделирования угроз.

Моделирование угроз защищаемой информации предусматривает выявление угроз путем анализа защищенности источников информации, определенных на предыдущем этапе, оценки опасности выявленных угроз и возможности их реализации в рассматриваемых условиях, а также определение величины потенциального ущерба от рассмотренных угроз. Моделирование завершается ранжированием угроз по величине потенциального ущерба. Угрозы с максимальным потенциальным ущербом создают наибольшую опасность информации и выбор мер по их нейтрализации составляют первоочередные задачи следующего этапа.

Рациональный выбор мер инженерно-технической защиты информации представляет собой совокупность эвристических процедур по определению вариантов мер нейтрализации рассматриваемой угрозы из состава рекомендуемых. Для каждой из выбранных мер определяются затраты на ее реализацию с учетом расходов в течение жизненного цикла (от момента реализации до пре-

кращения функционирования меры). Окончательный выбор меры из нескольких вариантов осуществляется по критерию «эффективность/стоимость». Выбор мер по нейтрализации каждой последующей меры завершается в момент, когда достигается требуемый уровень безопасности информации или исчерпывается выделенный на защиту ресурс системы. Однако при выполнении второго условия этот процесс целесообразно продолжить с целью определения дополнительного ресурса, необходимого для обеспечения требуемого уровня безопасности информации.

Особенностью алгоритма проектирования системы инженерно-технической защиты информации является наличие обратной связи. Обратная связь указывает на необходимость коррекции моделей объектов защиты и угроз информации с целью учета связей между угрозами и мерами защиты.

2. Исходные данные для моделирования объектов защиты содержатся в перечне сведений, составляющих государственную и коммерческую тайну. С целью определения источников защищаемой информации проводится структурирование информации, содержащейся в перечне сведений. Структурирование информации представляет собой процесс детализации на каждом уровне иерархической структуры, соответствующей структуре организации, содержания сведений (тематических вопросов) предыдущего уровня. Моделирование источников информации включает описание пространственного расположения источников информации и факторов, влияющих на защищенность информации, содержащейся в источниках. Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации — планов помещений, этажей зданий, территории в целом. Модель объектов защиты представляет собой набор чертежей, таблиц и комментарий к ним. Они содержат полный перечень источников защищаемой информации с оценкой ее цены, описание характеристик, влияющих на защищенность информации, мест размещения и нахождения ее информации, а также описание потенциальных источников опасных сигналов в местах нахождения источников информации.

3. Наиболее сложные задачи проектирования системы — определение источников угроз и анализ их возможностей. Для выявления угроз информации используются информативные демаски-

рующие признаки их источников — индикаторы угроз. В качестве индикаторов угроз воздействия на источники информации выступают действия злоумышленников и иных физических сил, а также условия, способствующие этим действиям, которые могут привести к их контакту с источниками защищаемой информации. В качестве индикаторов технических каналов утечки информации используются значения характеристик каналов утечки, которые создают реальные возможности разведывательного контакта носителя (защищаемой информацией) с злоумышленником.

Возможность реализации угрозы проникновения злоумышленника к источнику информации оценивается по значению произведения вероятностей двух зависимых событий: безусловной вероятности попытки к проникновению и условной вероятности преодоления им всех рубежей на пути движения его от точки проникновения до места непосредственного контакта с источником информации — вероятностью проникновения. В первом приближении вероятность угрозы воздействия аппроксимируется произведением двух экспоненциальных зависимостей, первая из которых описывает связь вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание, а вторая — зависимость вероятности реализации угрозы от соотношения времен движения злоумышленника и реакции системы на вторжение в случае его обнаружения. Более точные результаты могут быть получены в результате моделирования путей проникновения с помощью семантических цепей. В этой сети узел соответствует одному из рубежей и одной из контролируемых зон организации, а ребро — вероятности и времени перехода источника угрозы от одного рубежа (зоны) к другому (другой).

Обнаружение и распознавание технических каналов утечки информации производится по их демаскирующим признакам — индикаторам. Выявленные технические каналы утечки информации исследуются с помощью их моделей.

4. Риск утечки информации по оптическим каналам утечки информации оценивается в соответствии с количеством и точностью измерения видовых демаскирующих признаков объектов наблюдения. От них зависит вероятность обнаружения и распознавания объектов защиты. Существующие методики определения вероятности обнаружения и распознавания объектов наблюдения в

видимом свете учитывают большое количество факторов: контраст объекта по отношению к фону; линейные размеры объекта, его периметр, площадь; коэффициент, учитывающий форму объекта; расстояние от средства наблюдения до объекта; задымленность среды; характеристики средства наблюдения и др. Одним из основных факторов является количество пикселей изображения объекта наблюдения. Вероятность обнаружения и распознавания объектов наблюдения характеризует риск утечки информации по оптическому каналу.

5. Риск утечки речевой информации по акустическому каналу оценивается по громкости речи в точке подслушивания и более точно — по разборчивости речи в этой точке. Громкость речи измеряется инструментальными методами или рассчитывается по известным формулам, учитывающим громкость источника речевого сигнала, звукоизоляцию среды, вид приемника (человек или акустический приемник), мощность помех в точке приема. По упрощенным методикам громкость оценивается на частоте 1000 Гц, более точные результаты получаются при учете неравномерности спектров речевого сигнала и шума, размеров и неоднородности ограждений и амплитудно-частотных характеристик среды и уха. Наиболее точные оценки качества добываемой речевой информации обеспечиваются с помощью формантной, слоговой, словесной и фразовой разборчивости речи. Риск утечки речевой информации по акустическому каналу удобно на качественном уровне характеризовать градациями понятности речи.

6. Долю информации источника, попадающей к злоумышленнику в результате утечки по радиоэлектронному каналу, можно оценить по вероятности приема элемента информации, например символа сообщения, приемником злоумышленника, а также по пропускной способности канала. Так как вероятность ошибки или правильного приема зависит от отношения сигнал/шум на входе приемника, то риск утечки можно оценить также по величине этого отношения. Отношение сигнал/шум в месте возможного размещения приемника злоумышленника рассчитывается для конкретных параметров источника опасных радио- и электрических сигналов, дальности, затухания среды и прогнозируемых технических параметров приемника.

7. Для оценки показателей эффективности защиты информации использование количественных шкал затруднено, так как отсутствуют формальные методы определения показателей и достоверные исходные данные. Человечеством накоплен опыт решения слабоформализуемых задач, к которым относятся задачи оценки эффективности защиты информации, эвристическими методами, которые учитывают способности и возможности лица, принимающего решение (ЛПР). Объективность оценок ЛПР в условиях недостаточной и недостоверной информации выше при использовании им качественных шкал, чем количественных, причем число градаций качественной шкалы находится в пределах 5–9.

Градации качественной шкалы можно представить в виде алгебраического выражения $x^n y$, где x обозначает базовое значение лингвистической переменной (показателя эффективности), n — числа натурального ряда (показатели x), а y — наименование лингвистической переменной (показателя эффективности). В качестве базового значения лингвистической переменной принимаются значения «большой(ая)», «высокий(ая)». Значения композиции лингвистических переменных определяются путем сложения (при умножении лингвистических переменных) или вычитания (при их делении).

8. Рекомендации по повышению уровня физической защиты источников информации совпадают с рекомендациями по физической защите иных материальных ценностей. Максимальное укрепление периметра организации предусматривает создание инженерных конструкций высотой не менее 2,5 м с козырьком по верху ограждения из 3–4 рядов оцинкованной проволоки. С внутренней стороны ограждения устанавливается зона отторжения шириной не менее 3 м и предупредительное ограждение. В зоне отторжения размещаются средства обнаружения и наблюдения, охранное и дежурное освещение, постовые грибки со связью для охраны, разграничительные и указательные знаки, а для обнаружения следов злоумышленников создается контрольно-следовая полоса. Предупредительные ограждения высотой не менее 1,5 м из металлической сетки, проволоки, досок (штакетники) затрудняют проникновение на контрольно-следовую полосу сотрудников организации и животных.

Входные деревянные двери должны иметь толщину не менее 40 мм, а двери, выходящие во двор организации, чердаки и подва-

лы, а также в места хранения материальных ценностей, обиваются с двух сторон оцинкованной сталью толщиной не менее 0,6 мм с загибом краев листа на торцы дверного полотна. Дверные коробки зданий и помещений выполняются из стального профиля или дерева, усиленного стальными уголками размером 30 × 40 × 5 мм. Помещения, в которых размещаются материальные ценности, могут оборудоваться с внутренней стороны дополнительными решетчатыми раздвижными или распашными дверями с ушками для навесного замка. Оконные проемы на первых этажах зданий, вблизи пожарных лестниц, над козырьками заборов и примыкающими строениями оборудуются стационарными или съемными раздвижными (распашными) решетками или ставнями. Также стационарными или раздвижными (распашными) решетками защищаются витринные проемы зданий. Глухими решетками защищаются теплопроводы, дымоходы, вентиляционные шахты и вентиляционные короба размером более 200 × 200 мм.

9. На рубежах охраны технические средства обнаружения выбираются с учетом вида рубежа, способов обнаружения злоумышленника и пожара, а также значений их конкретных тактико-технических характеристик (ТТХ). При выборе типа извещателя учитываются вид охраняемого рубежа или зоны, их размеры и конфигурация, вид воздействия злоумышленника на преграду, затраты на приобретение, установку (строительство) и эксплуатацию инженерных конструкций и технических средств. Размеры охраняемой зоны (площадь, длина) технического средства должны в 1,1–1,4 раза превышать реальные. Количество шлейфов на каждом рубеже определяется его конфигурацией и протяженностью. Для охраны периметра рекомендуются шлейфы для фасада, тыла, правой и левой сторон. Для обеспечения круглосуточной пожарной охраны ее средства и средства охранной сигнализации соединяются с приемно-контрольным пунктом раздельными шлейфами. Для нейтрализации подготовленного злоумышленника целесообразна установка на возможном пути его следования скрытных ловушек.

Телевизионные камеры устанавливают в местах с максимальной потенциальной угрозой с учетом вида наблюдения (скрытого или открытого), геометрических размеров зоны охраны и ее освещенности в разное время суток, информативных демаскирующих признаков, условий эксплуатации. Кроме того, при выборе мес-

та установки камеры обращается внимание на необходимость исключения засветки камеры внешним светом. Фокусное расстояние объектива камеры выбирается исходя из требуемого угла зрения, геометрических размеров охраняемой зоны, требуемого для идентификации объектов наблюдения разрешения. Для увеличения зоны наблюдения применяют поворачивающие платформы камер, а для повышения разрешения — объективы с переменным фокусным расстоянием.

10. Для защиты информации от наблюдения через окна помещений в них уменьшают освещенность объектов и прозрачность окон путем применения занавесок, штор, жалюзи, тонированных окон и пленок на окиах, для предотвращения наблюдения через приоткрытую дверь на нее устанавливают доводчик дверей и самозащелкивающиеся замки. Для исключения несанкционированного получения информации с экранов мониторов компьютеров мониторы размещают в местах, исключающих возможность наблюдения экранов посторонними лицами, а интервал включения заставки на экране монитора выбирается минимальным. Маскировки объектов защиты на открытых площадках обеспечивается с помощью искусственных масок, маскировочного окрашивания, дымов и пены, ослепления наблюдателя (злоумышленника или светоэлектрического преобразователя средства наблюдения) с помощью ярких источников света, попадающих на изображение объекта (засветка) и поле изображения, а также создания ложных объектов прикрытия. В качестве мер защиты от радиолокационного наблюдения рекомендуется: установка на объектах защиты искусственных масок, изменяющих направление отражения падающей электромагнитной волны радиолокатора; размещение на объектах защиты или среди объектов фона радиоотражающих средств; излучение помех, имитирующих ложные объекты.

11. Для защиты информации от подслушивания через дверь целесообразно устранить щели между дверным полотном и рамой, заменить дверь на более тяжелую (с большей поверхностной массой), покрыть дверь звукопоглощающим материалом, установить вторую дверь с тамбуром. Для автоматического прикрытия двери на ней укрепляется доводчик дверей и замок с автоматической защелкой. Для исключения утечки речевой информации через откры-

тое окно его закрывают, устанавливают звукоизолирующие прокладки между оконными рамами, закрывают окно плотными шторами, добавляют третью раму, создают виброакустическое зашумление стекол окна. Если стена помещения имеет недостаточную звукоизоляцию, то ее толщину и поверхностную массу увеличивают путем дополнительной кирпичной кладки и установки акустических экранов, покрывают стену звукопоглощающими материалами, создают виброакустическое зашумление стены. Для предотвращения утечки речевой информации через вентиляционное отверстие устанавливают перед ним экран, в случае недостаточности его звукоизоляции укрепляют внутри его глушитель. Для защиты информации в каналах связи необходимо соблюдать дисциплину связи, обеспечить техническое закрытие электро- и радиосигналов и шифрование сообщений. Для предотвращения утечки речевой информации через ПЭМИН выключают все незащищенные радиоэлектронные средства и электрические приборы, включают между работающими средствами и линиями связи устройства фильтрации и уменьшения малых амплитуд опасных сигналов, буферные устройства, экранируют радиоизлучающие ОТСС, кабели и провода линий связи и электропитания, создают линейное и пространственное зашумление опасных сигналов.

12. Для предотвращения подслушивания с помощью закладных устройств применяются средства поиска, обнаружения и локализации закладных устройств по их радио- и электрическим сигналам, по наличию в местах возможного размещения закладных устройств полупроводниковых и металлических элементов, путем просвечивания средств и стен устройствами рентгеноскопии, пространственного и линейного зашумления среды распространения сигналов закладных устройств. Поиск закладных устройств целесообразно проводить в три этапа: подготовительный, этап проведения поисковых мероприятий и заключительный. Подготовительный этап предусматривает: прогноз вероятного противника и анализ его оперативно-технических возможностей; изучение помещения и его окружения; определение находящихся в помещении предметов, радиоэлектронных средств, электрических приборов, кабелей информационных линий и цепей электропитания; изучение планов и схем помещения и коммуникаций; установку фактов и характера

работ, проводимых в помещении; определение методик поисковых мероприятий и перечня поисковой аппаратуры; разработку легенды поиска и вариантов поведения поисковой бригады. Поисковые мероприятия в помещении начинаются с его визуального осмотра. Затем последовательно или параллельно производится проверка предметов интерьера и мебели, коммуникаций, специальные исследования радиоэлектронных средств. На заключительном этапе поисковых мероприятий готовятся отчетные документы со схемами и описанием мест срабатывания аппаратуры, вскрытий участков стен, предметов мебели и интерьера, аппаратуры. Отчет завершается оценкой состояния защищенности информации и рекомендациями по его усилению.

13. Меры по защите информации по вещественному каналу различаются в зависимости от вида защищаемой информации. Для защиты семантической информации и видовых признаков собирают, учитывают и уничтожают отходы производства, физически стирают информацию на магнитных носителях информации. Для предотвращения утечки демаскирующих признаков внедряют безотходные технологии, производят чистку путем фильтрации, охлаждения, нагревания и химических реакций отходов, содержащих демаскирующие вещества, а также захоронение отходов, с демаскирующими веществами.

## Литература к разделу V


1. *Варламов А. В., Кисиленко Г. А., Хорев А. А., Федоринов А. Н.* Технические средства видовой разведки / Под редакцией *А. А. Хорева*. — М.: РВСН, 1997.
2. *Василевский И. В., Болдырев А. И.* Облава на «жучков»? Мы знаем, как это сделать // Конфидент. — 2000. — № 4–5. — С. 96–105.
3. *Волобуев С. В.* Безопасность социологических систем. — Обнинск: Викинг, 2000.
4. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений. — М.: Мир, 1976.
5. Организация проведения поисковых мероприятий. Специальная защита объектов. — М.: Росси, 1997.
6. Руководящий нормативный документ. Системы комплексы охранной сигнализации. Элементы технической укрепленности объектов. Нормы проектирования. РД 78.143-92. МВД России. — М.: Издание официальное, 1992.

## Заключение

Парадокс любого развития состоит в том, что его достижения имеют побочные негативные последствия. Прогресс в информационных технологиях создает одновременно проблему необходимости обеспечения информационной безопасности. Это противоборство непрерывно и бесконечно. Достижения в информационных технологиях требуют новых решений для обеспечения инженерно-технической защиты информации. Поэтому проблему обеспечения информационной безопасности не удастся закрыть раз и навсегда. Важно, чтобы новые меры по инженерно-технической защите информации не противоречили известным, а их дополняли. Это возможно, если основу знаний по инженерно-технической защите составляет не совокупность данных, даже систематизированных, по защите информации, а ее теория. Только теория может ответить на вопросы: что, от кого или чего и как надо защищать в конкретных условиях не только сегодня, но и завтра.

Первоочередной вопрос теории — сущность и свойства защищаемой информации. Конечно, все более широко распространяемое представление об информации в виде самостоятельно существующей субстанции или части единого мирового информационного поля поражает воображение людей и является привлекательным не только для лириков, но и физиков. Но для решения сугубо прагматических задач, к каким относится защита информации, такая модель не конструктивна, ибо нельзя защищать нечто, которое невозможно, образно говоря, «потрогать». В результате анализа в данной книге сущности информации с позиции защиты ореол ее как чего-то особенного и не очень понятного существенно поблек. Информация представляется лишь как совокупность значений признаков материальных объектов, которые при взаимодействии с другими объектами изменяют свои признаки и признаки других объектов. При изменении собственных признаков носителя информации происходит ее изменение или уничтожение, при изменении признаков других объектов под признаки носителя информации — копирование информации. Если копирование санкционировано, то речь идет о передаче информации, если не санкционировано, имеет место хищение информации. Количество передаваемой информации характеризуется мерой изменения признаков взаимодейству-

ющих объектов. Так как каждый объект имеет свой набор значений признаков, то не может быть объективной меры для количества информации.

При таком подходе для защиты информации, содержащейся в признаках объекта-носителя, необходимо исключить взаимодействие этого объекта с другими. Проблема защиты усложняется из-за того, что информацию нельзя на долгое время, как, например, драгоценный камень, запереть в сейфе. Во-первых, со временем изменяются признаки получателей информации — информация стареет, а во-вторых, информация полезна, когда используется. Однако «работающая» информация способна, как энергия в замкнутом пространстве, растекаться в пространстве. Вследствие этого необходимы дополнительные и немалые усилия, чтобы задержать ее несанкционированное распространение. Возможность объекта — носителя информации изменять признаки других взаимодействующих объектов без заметных изменений своих признаков также усложняет задачу своевременного обнаружения хищения информации путем ее копирования.

В соответствии с таким подходом семантическую информацию можно рассматривать как представление информации, содержащейся в значениях признаков объектов, на языке символов. Кодирование осуществляет вторая сигнальная система человека для обеспечения процессов мышления. Семантическая информация является вторичной по отношению к информации, содержащейся в признаках объектов. Независимо от вида информации (признаковой или семантической) материальным объектом защиты является носитель признаков.

Угрозы информации в соответствии с рассматриваемой теорией инженерно-технической защиты информации обусловлены потенциальной возможностью как воздействия объектов на носитель информации, так и воздействием носителя информации на другие объекты. Источниками угроз являются люди и природные явления. Угрозы можно разделить на угрозы, при реализации которых внешние силы изменяют информационные параметры носителя информации, и угрозы, приводящие к ее копированию в результате воздействия носителя на иные объекты. Первая группа угроз названа угрозами воздействия, вторая — угрозами утечки.

Угрозы воздействия могут быть преднамеренными и случайными. Преднамеренные угрозы информации создают люди, случайные угрозы возникают в результате сбоев в работе технических средств, ошибок людей, действий стихийных сил. Возможности несанкционированного распространения носителя с информацией от ее источника к злоумышленнику зависят от вида носителей информации и показателей технических каналов утечки информации. По виду носителя информации различают оптические, акустические, радиоэлектронные и вещественные каналы утечки. Каналы утечки информации характеризуются пропускной способностью, длиной и относительной информативностью.

В соответствии с такими моделями объектов защиты и угроз теория инженерно-технической защиты позволяет свести многообразие методов к защите информационных параметров носителей информации от внешних сил воздействия и от несанкционированного копирования — хищения информации. Первая группа методов обеспечивает физическую защиту информации от внешних сил путем затруднения движения источников угроз к источникам информации, обнаружения источников угроз и их своевременную нейтрализацию. Вторая группа методов предотвращает несанкционированное копирование информации за счет пространственного, временного, структурного и энергетического скрытия информации и ее носителей.

Реализация методов в конкретных условиях достигается с помощью разнообразных технических средств. Наибольший эффект достигается, когда силы и средства, обеспечивающие достижение целей и решение задач информационной безопасности, образуют систему защиту информации. Входами системы являются угрозы, выходами — меры по их предотвращению и нейтрализации. В соответствии с двумя группами методов и соответствующих технических средств система инженерно-технической защиты информации состоит из подсистемы физической защиты источников информации и подсистемы скрытия информации и ее носителей. Эти подсистемы включают комплексы инженерной защиты, технической охраны, защиты от подслушивания, наблюдения, перехвата сигналов, предотвращения утечки информации по вещественному каналу и комплекс управления. Особенностью системы инженер-

но-технической защиты информации является то, что она не создается автономно, а представляет собой модель, позволяющую решать задачи по инженерно-технической защите информации с позиций системного подхода путем эффективного использования сил и средств ресурса, выделенного на защиту информации.

Защиту информации, содержащей государственную тайну, обеспечивает государственная система защиты информации от технической разведки. Силы государственной системы защиты информации образуют пирамиду, наверху которой находятся Межведомственная комиссия по защите государственной тайны, Федеральная служба по техническому и экспортному контролю РФ и Федеральная служба безопасности РФ, внизу — органы безопасности на предприятиях (в организациях и учреждениях). Нормативно-правовую базу государственной системы защиты информации составляют руководящие, нормативные и методические документы федерального, ведомственного и учрежденческого уровней. Защиту коммерческой и других тайн обеспечивает их владелец. Эффективная защита информации достигается комплексным применением организационных, инженерно-технических и программно-аппаратных мер по защите и их постоянным контролем.

Проектирование (совершенствование) системы инженерно-технической защиты информации проводится в три последовательных этапа, основу которых составляют моделирование объектов защиты, моделирование угроз информации и выбор рациональных мер по ее защите. Моделирование предусматривает описание источников информации и угроз ей на естественно-профессиональном и математическом языках и анализ моделей для конкретных условий. Меры защиты информации от каждой угрозы выбираются по критерию эффективность/стоимость до момента, когда суммарные затраты на них не превысят выделенный ресурс. Такой алгоритм построения (совершенствования) системы инженерно-технической защиты информации позволяет определить не только комплекс рациональных мер, но и оценить уровень безопасности информации при выделенном ресурсе, а также ресурс, необходимый для обеспечения требуемого уровня безопасности. Для оценки показателей эффективности угроз информации и мер по ее за-

щите предлагается качественная шкала измерений показателей и аппарат их преобразований (умножения и деления).

Так как эффективность выбираемых мер по защите информации в значительной мере зависит от умения и практических навыков соответствующих специалистов, то при изучении инженерно-технической защиты информации большое внимание должно уделяться практическим занятиям по единому сценарию, отражающему основные вопросы защиты конкретных объектов. Необходимую для этого нормативно-методическую базу создают приведенные в приложении сценарий защиты информации в кабинете руководителя организации и технические характеристики средств добывания и инженерно-технической защиты информации.

Изложенный в книге материал по инженерно-технической защите информации охватывает вопросы (дидактические единицы) специальностей по информационной безопасности. Однако изложение материала по уровням знаний позволяет достаточно гибко формировать учебные курсы как с учетом меньшего количества выделенных часов общеобразовательных стандартов, так и уровня подготовки и круга должностных функциональных обязанностей специалистов на курсах повышения квалификации в сфере инженерно-технической защиты информации.

## Основные используемые термины и понятия

**Активность защиты информации** — упреждающее предотвращение (нейтрализация) угроз безопасности информации.

**База сигнала** — произведение ширины полосы спектра сигнала на время его передачи.

**Безопасность информации** — состояние защищенности информации, при котором обеспечивается допустимый риск ее уничтожения, изменения, хищения и блокирования.

**Биометрическая идентификация** — идентификация, основанная на использовании индивидуальных признаков человека.

**Вспомогательные технические** средства и системы (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения защищаемой информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

**Геосинхронная орбита КА** — орбита КА, плоскость которой соответствует плоскости экватора Земли, а период вращения КА равен периоду вращения Земли вокруг оси. КА на такой орбите «висит» на высоте около 37 тысяч км над определенной точкой экватора Земли.

**Георадар** — станция подповерхностной радиолокации.

**Геофон** — преобразователь акустического сигнала, распространяющегося в земной поверхности, в эквивалентный электрический.

**Гибкость защиты информации** — возможность оперативно изменять меры защиты.

**Гидрофон** — преобразователь акустического сигнала, распространяющегося в водной среде, в эквивалентный электрический.

**Государственная тайна** — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

**Демаскирующее вещество** — вещество, содержащее демаскирующие вещественные признаки объекта защиты или технологию его изготовления.

**Демаскирующий признак** — признак объекта, позволяющий отличить его от других объектов.

**Длина технического канала утечки информации** — расстояние от источника сигнала (информации) до приемника сигнала (получателя), на котором обеспечивается допустимое качество информации, добываемой злоумышленником.

**Доступ** — возможность контакта субъекта и объекта с источниками информации.

**Доступ санкционированный (несанкционированный)** — разрешенный (неразрешенный) контакт субъектов и объектов с источниками информации.

**Закладное устройство** — радиоэлектронное средство для добывания информации, устанавливаемое (размещаемое) скрытно.

**Злоумышленник** — лицо или организация, добывающие информацию незаконным путем.

**Идентификатор доступа** — демаскирующий признак субъекта и объекта, по которому принимается решение о доступе.

**Инструментальные методы контроля** — методы контроля с использованием контрольно-измерительных приборов.

**Информация** — совокупность значений характеристик материального объекта.

**Информация признаковая** — информация, отображаемая на языке признаков.

**Информативность источника информации** — полнота ответа, содержащегося в информации источника, на интересующие злоумышленника (орган добывания) вопросы.

**Информативность демаскирующего признака** — мера индивидуальности демаскирующего признака объекта.

**Информация закрытая** — информация, содержащая государственную, коммерческую или иную тайну.

**Информация секретная** — информация, содержащая государственную тайну.

**Информация конфиденциальная** — служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной тайне, государственной службе и других законодательных актов.

**Информационный портрет объекта защиты** — описание объектов защиты в виде структуры его информационных элементов.

**Источники информации** — субъекты и объекты, от которых может быть получена информация.

**Источники семантической информации** — субъекты и объекты, от которых может быть получена информация с характеристиками (реквизитами), позволяющая оценить ее достоверность.

**Количество информации** — мера изменения признаков объекта после его взаимодействия с другими объектами.

**Контролируемая зона** — часть пространства, в которой обеспечивается контроль безопасности информации.

**Многозональность инженерно-технической защиты информации** — разделение пространства, в которой находятся источники защищаемой информации, на зоны, уровень защиты информации в которой соответствует ее цене.

**Многорубежность инженерно-технической защиты информации** — наличие на пути распространения источников угроз преград, уменьшающих энергию источников угроз и увеличивающих время их движения.

**Надежность защиты информации** — состояние защищенности информации, соответствующее определенному уровню ее безопасности.

**Непрерывность защиты информации** — постоянная готовность системы защиты информации к предотвращению (нейтрализации) угроз.

**Область рациональной защиты информации** — значения прямых расходов на защиту информации, при которых минимизируются суммарные (с учетом ущерба от реализации угроз) расходы на информацию.

**Объем сигнала** — характеристика сигнала, равная произведению ширины спектра сигнала, его динамического диапазона и времени передачи.

**Основные технические средства и системы** — технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи защищаемой (содержащей тайну) информации.

**Остронаправленный микрофон** — специальный микрофон для скрытного подслушивания, имеющий узкую диаграмму направленности.

**Относительная информативность канала утечки информации** — доля информации источника, которая может быть передана по каналу в случае ее утечки.

**Периодический контроль эффективности защиты информации** — контроль эффективности защиты информации, проводимый в заранее определенное время.

**ПЗС-матрица** — полупроводниковый преобразователь оптического изображения в электрический сигнал, формируемый путем последовательного считывания зарядов пикселей строк кадра.

**Побуждение** — создание у сотрудников установки на осознанное выполнение требований по защите информации.

**Постоянный контроль эффективности защиты информации** — контроль эффективности защиты информации, время проведения которого проверяемому неизвестно.

**Предварительный контроль эффективности защиты информации** — контроль эффективности системы защиты информации при изменениях ее состава, структуры и алгоритма функционирования.

**Признаковая структура** — упорядоченная совокупность признаков, принадлежащих одному объекту.

**Принуждение** — метод организации работы, предусматривающий выполнение требований под угрозой административной или уголовной ответственности.

**Пропускная способность технического канала утечки информации** — количество информации, передаваемой в единицу времени.

**Равнопрочность рубежа защиты информации** — отсутствие в рубеже защиты информации участков (мест) с прочностью менее допустимой.

**Регламентация** — установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленных на обеспечение безопасности информации.

**Риск утечки (наблюдения, подслушивания, перехвата)** — вероятность утечки информации от ее источника к злоумышленнику.

**Риск воздействия на источник информации** — вероятность физического контакта источника угрозы воздействия с источником информации, в результате которого информация может быть изменена, уничтожена или похищена.

**Сигнал** — динамический носитель информации.

**Сигнал опасный** — сигнал с закрытой информацией.

**Системный анализ** — комплекс методов и процедур, позволяющих выработать в результате анализа модели системы рациональные рекомендации по решению проблем системы.

**Система защиты информации** — модель системы, объединяющей силы и средства по защите информации и описываемой системными параметрами: целями и задачами, ресурсами, угрозами, мерами по их нейтрализации и процессом выбора рациональных мер защиты для конкретных угроз.

**Системный подход** — исследование объекта или процесса с помощью модели, называемой системой.

**Системное мышление** — форма мышления, характеризующая способность человека на бессознательном уровне решать задачи дедуктивным методом

**Слабоформализуемые задачи** — задачи, не имеющие формальных постановки и оптимального решения.

**Скрытие информации** — совокупность методов, затрудняющих обнаружение и распознавание объектов защиты злоумышленниками и их техническими средствами.

**Скрытие пространственное** — метод защиты информации, предусматривающий размещение источников информации в местах, неизвестных злоумышленникам.

**Скрытие временное** — метод защиты информации путем исключения проявления демаскирующих признаков объекта защиты во время действий злоумышленников и их средств по добыванию информации.

**Скрытие структурное** — изменение информационного портрета объекта защиты под информационные портреты фона, или объектов прикрытия.

**Скрытие энергетическое** — уменьшение отношения сигнал/шум на входе приемника злоумышленника до значений, при которых качество добываемой информации становится неприемлемым.

**Скрытность защиты информации** — скрытное проведение мер по защите информации и существенное ограничение допуска к информации о конкретных способах и средствах инженерно-технической защиты информации.

**Стетоскоп** — преобразователь акустического сигнала, распространяющегося в твердой среде, в эквивалентный электрический сигнал.

**Технический контроль эффективности защиты информации** — методы контроля эффективности защиты информации, предусматривающие определение уровней опасных сигналов.

**Точка доступа** — место, где осуществляется контроль доступа.

**Чувствительность** — характеристика приемника, позволяющая оценить способность приемника принимать сигналы малой мощности.

**Чувствительность предельная** — характеристика приемника, значение которой равно уровню шумов его входных цепей.

**Чувствительность реальная** — характеристика приемника, значение которой соответствует минимальному уровню сигнала на входе приемника, при котором обеспечивается определенное отношение сигнал/шум на его выходе.

**Управление нормативное** — управление силами и средствами объекта управления в соответствии с планом.

**Управление оперативное** — управление силами и средствами объекта управления с учетом конкретной обстановки.

**Целеустремленность защиты информации** — сосредоточение ресурса системы на предотвращении (нейтрализации) наиболее ценной информации.

**Цена информации** — полезность информации для участников информационного рынка.

**Ценность информации** — полезность информации для ее владельца (пользователя).

**Эффективность защиты информации** — мера соответствия уровня безопасности информации требованиям при заданном ресурсе на ее защиту.

**Элемент признаковой информации** — информация, содержащаяся в одном именном признаке объекта.

**Эффективная поверхность рассеяния (отражения)** — площадь металлической поверхности гипотетического объекта, который равномерно отражает во все стороны электромагнитную волну радиолокационной станции, а помещенный в место нахождения реального объекта создает у приемной антенны радиолокационной станции такую же плотность потока мощности, как и реальный объект.

# Сценарий инженерно-технической защиты информации в кабинете руководителя организации

Сценарий предназначен для формирования на практических занятиях навыков по обеспечению защиты информации в кабинете руководителя организации. В сценарии рассматриваются все основные этапы и процедуры защиты информации по темам:

- моделирование кабинета руководителя как наиболее сложного объекта защиты;
- моделирование угроз информации в кабинете руководителя организации;
- выбор рациональных мер по защите информации в кабинете руководителя организации.

## 1. Моделирование кабинета руководителя организации как объекта защиты

### 1.1. Обоснование выбора кабинета как объекта защиты

Выбор кабинета как объекта защиты обусловлен следующими факторами:

- в кабинете руководителя циркулирует наиболее ценная информация организации;
- кабинет посещают сотрудники организации всех должностных категорий по служебным и личным вопросам, а также посетители организации;
- в кабинете, как правило, размещаются различные радио- и электрические приборы, которые могут быть источниками побочных электромагнитных излучений и наводок;
- в кабинете во время докладов и совещаний проводится демонстрация продукции, документов, плакатов, аудио- и видеоматериалов;
- в кабинете много элементов интерьера и мебели, в которой легко спрятать закладные устройства.

Кабинет руководителя, как правило, граничит с приемной и другими служебными помещениями. В приемной возможно длительное присутствие посторонних лиц (сотрудников и посетителей), ожидающих приема. В результате недостаточной зашиты информации в кабинете (например, из-за слабой звукоизоляции стены), относительно частого открывания двери в кабинет, продолжения в приемной разговора на служебные темы выходящих из кабинета людей, работы секретаря с документами в присутствии находящихся в приемной людей могут создаться реальные предпосылки для утечки информации из приемной.

Во время совещания с участием представителей других организаций или беседы руководителя с посетителями последние могут попытаться записать конфиденциальный разговор с помощью скрытной записи на диктофон или закладного устройства с целью последующего использования этой информации во вред руководителю организации или организации в целом.

Здание, в котором находится кабинет, как правило, окружено другими административными и жилыми домами, через окна и с крыши которых возможно наблюдение за источниками информации в кабинете, а также возможен перехват из кабинета радиосигналов закладных устройств и побочных электромагнитных излучений и наводок.

Следовательно, кабинет представляет собой объект защиты, в котором, с одной стороны, циркулирует наиболее ценная информация, а с другой стороны, возможен доступ в него всех категорий сотрудников и посетителей, в том числе тех, которые могут заниматься добыванием информации.

## 1.2. Характеристика информации, защищаемой в кабинете руководителя

### *1.2.1. Виды информации в кабинете руководителя*

В кабинете руководителя могут находиться на различных носителях почти все виды защищаемой в организации информации, в том числе:

- семантическая информация в документах, с которыми работает руководитель или которые приносят его заместители, дру-

гие сотрудники, представители других организаций, а также на чертежах и плакатах, развешиваемых на стенах или проецируемых во время докладов и совещаний;

- семантическая речевая информации во время конфиденциального разговора руководителя с посетителями и выступлений участников совещания;
- информация о видовых признаках VIP-персон, посещающих руководителя и по характеру деятельности которых можно определить тематику обсуждаемых вопросов;
- видовые демаскирующие признаки продукции, макетов и опытных образцов, которые демонстрируются руководителю на разных этапах их производства, а также их изображения на плакатах, экранах видеопроектора или телевизора;
- демаскирующие признаки веществ, приносимых руководителю для демонстрации соответствующей продукции, а также образцы исходных материалов.

Основными видами информации в кабинете руководителя являются: речевая информация, семантическая информация на плакатах и экране видеопроектора, информация о видовых демаскирующих признаках продукции.

### *1.2.2. Источники информации в кабинете руководителя*

Основными источниками информации в кабинете руководителя являются:

- руководитель организации;
- должностные лица организации, посещающие кабинет;
- представители других организаций, с которыми руководитель обменивается секретной (конфиденциальной) информацией в ходе встреч или совещаний;
- посетители во время приема по личным вопросам, разговор с которыми может содержать сведения, содержащие коммерческую или иную тайну;
- документы на столах, плакаты на стенах, аудио- и видеодокументы;
- приносимая в кабинет продукция, сведения о которой и ее демаскирующие признаки содержат государственную, коммерческую или иную тайну;

- приносимые в кабинет материалы и продукция в виде веществ, информация о составе и технологии изготовления которых защищается.

Характеристика информации и ее источников дана в табл. П.1.1.

*Таблица П.1.1*

| *№ п/п* | *Вид информации в кабинете* | *Источник информации* | *Максимальная цена информации* | *Место нахождения источника информации в кабинете* |
|---|---|---|---|---|
| 1 | Семантическая документальная | Документы | Очень высокая | В сейфе, на столах, на плакатах, на стене, на экране монитора, плакатах, доске, экране видеопроектора |
| 2 | Семантическая речевая акустическая | Люди | Очень высокая | В кабинете |
| 3 | Семантическая речевая, читаемая по губам | Люди | Средняя | В кабинете |
| 4 | Видовые признаки | Продукция | Средняя | На столе, изображения на плакатах, экране монитора, телевизора, видеопроектора |
| 5 | Видовые признаки | Люди | Низкая | В кабинете |
| 6 | Видовые признаки | Вещества и материалы | Очень низкая | На столах |
| 7 | Вещественные признаки | Продукция: | | |
| | | — химического производства; | Средняя | На столах |
| | | — других производств | Низкая | На столах |
| 8 | Вещественные признаки | Материалы | Очень низкая | На столах |

Продукция, сигналы которой содержат защищаемые сигнальные признаки, во время ее демонстрации в кабинете не включается во избежание утечки информации. Поэтому информация о сиг-

нальных демаскирующих признаках разрабатываемой продукции в сценарии не рассматривается.

При определении цены защищаемой в кабинете руководителя информации используется качественная шкала с 5 градациями: очень высокая, высокая, средняя, низкая, очень низкая. Для конкретизации этих лингвистических значений уточняются граничные значения «очень низкая» и «очень высокая»:

- очень высокая — цена информации, утечка которой может нанести государству очень большой ущерб или привести к банкротству фирмы;
- очень низкая — цена информации, потеря которой не имеет последствий.

С учетом этого остальные значения цены информации принимают следующее градации:

- высокая — цена информации, утечка которой может нанести государству большой ущерб или заметно ухудшить финансовое положение фирмы;
- средняя — цена информации, потеря которой может привести к существенным для государства и фирмы финансово-экономическим потерям, но может компенсироваться внутренними резервами фирмы;
- низкая — цена информации, утечка которой приводит к малым потерям.

Для государственных структур признаком цены информации может служить ее гриф секретности: «чрезвычайной важности» — чрезвычайно высокая, «совершенно секретно» — очень высокая, секретно — высокая, для «служебного пользования» — низкая.

Наибольшую цену имеет семантическая документальная информация. Цена информации о видовых и вещественных признаков зависит от их информативности. На предприятиях химический и смежных сфер промышленности цена информации о вещественных признаках продукции может быть высокой, так как состав веществ и технология их изготовления для этих предприятий является основной государственной или коммерческой тайной. Для машиностроительных предприятий цена такой информации низкая. Но могут быть исключения, например, если существенное улучшение параметров продукции достигнуто за счет применения новых материалов.

При формировании этой таблицы также важно указать все места нахождения источников информации в кабинете, так как они могут существенно влиять на величину угрозы канала утечки. Например, если документ находится на столе, то возможности его наблюдения через окно весьма ограничены, если он в виде плакате повешен на стену напротив окна, то риск наблюдения резко возрастает.

### 1.3. План кабинета как объекта защиты

Кабинет размещен на 3-м этаже 5 этажного кирпичного здания, примыкающего к тротуару улицы. Окна кабинета выходят на улицу. Ширина улицы составляет около 50 м. На противоположной стороне улицы расположены жилые 12 этажные дома. Территория организации обнесена бетонным забором высотой 2 м, соединенного с наружной стеной административного здания. Вход людей в организацию обеспечивается через контрольно-пропускной пункт (КПП), въезд автотранспорта — через ворота. Вход в здание через дверь, открываемую во двор. Окна 1-го этажа укреплены стальными решетками.

Схема расположения организации представлена на рис. П.1.1.

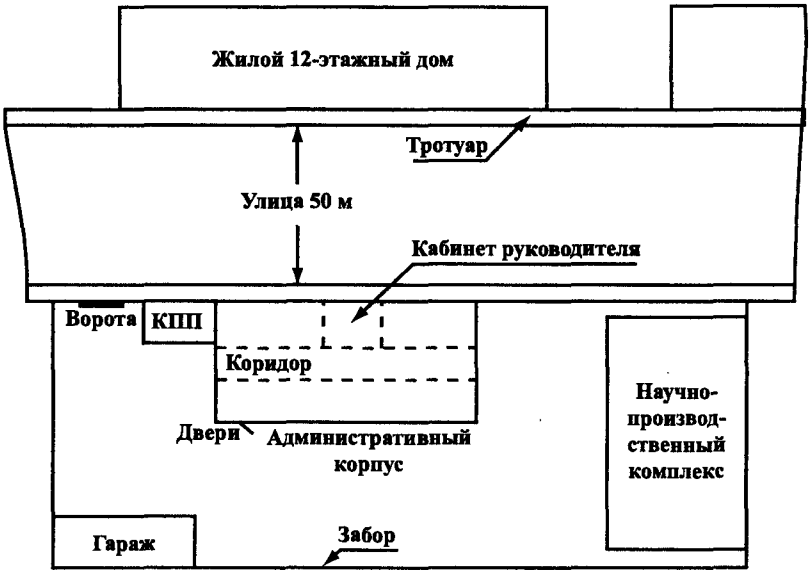



*Рис. П.1.1.* Схема расположения организации

Кабинет имеет два окна, выходящие на улицу, и дверь в приемную. Площадь кабинета составляет около 30 м$^2$, приемная 20 м$^2$. Схематический чертеж варианта кабинета приведен на рис. П.1.2.

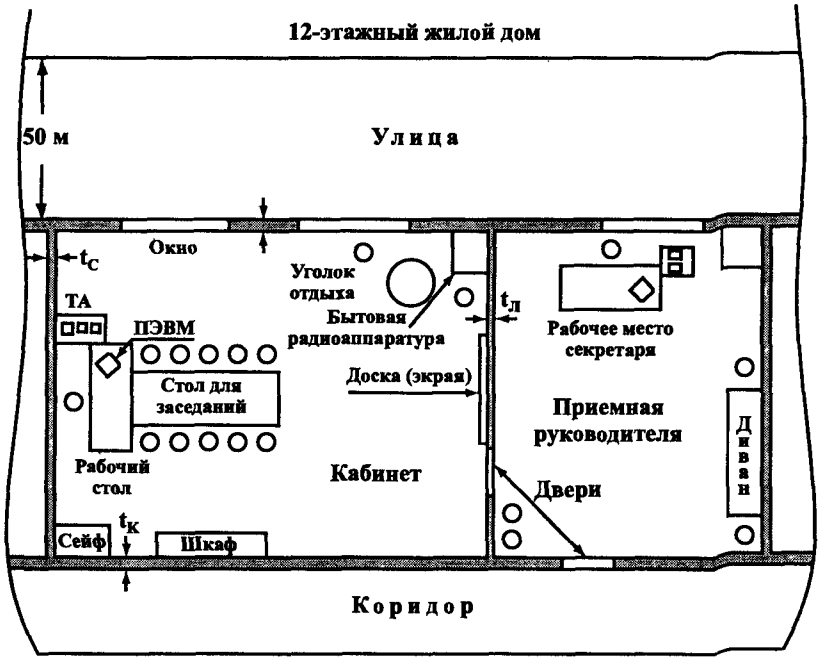



*Рис. П.1.2.* Модель кабинета руководителя

Для описания (моделирования) факторов, влияющих на защищенность информации в кабинете, проводится его обследование. Модель (описание) помещения содержит 5 групп факторов:

- общая характеристика помещения;
- ограждения;
- предметы мебели и интерьера;
- радиоэлектронные средства и электрические приборы;
- средства коммуникаций.

Результаты обследования помещены в табл. П.1.2.

*Таблица П.1.2*

| *№ п/п* | *Факторы влияния* | *Параметры* | *Примечание* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| **1** | **Общая характеристика помещения** | | |
| 1.1 | Этаж | 3 | |
| 1.2 | Площадь, м$^2$ | 30 | |
| 1.3. | Смежные помещения | справа — приемная;<br>слева — кабинет заместителя;<br>вверху — служебное помещение организации;<br>внизу — служебное помещение организации | |
| **2** | **Ограждения** | | |
| 2.1 | Стены | *наружная* — железобетонная толщиной 400 мм, на стене укреплены 2 чугунные батареи отопления, соединенные металлическими трубами с трубами в боковых стенах;<br>*смежная с коридором* — железобетонная толщиной 140 мм; 2 вентиляционных отверстия | |
| | | *смежная с приемной* — кирпичная толщиной в 1 кирпич (270 мм);<br>*смежная с кабинетом заместителя* — железобетонная толщиной 140 мм | |
| 2.2 | Потолок | железобетонная плита толщиной 400 мм, окрашенная водо-эмульсионной краской | |
| 2.3 | Пол | железобетонная плита толщиной 400 мм, покрытый паркетом и ковролином | |
| 2.4 | Окна | количество — 2, двухрамные, обращены на улицу, толщина стекла — 3 мм | |
| 2.5 | Дверь | типовая щитовая, без доводчика, выход в приемную | |
| **3** | **Предметы мебели и интерьера** | | |
| 3.1 | Картина | размеры рамы 700 × 500 мм, она повешена под углом к стене, смежной с коридором | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 3.2 | Шкаф книжный | дверцы стеклянные, на 4 полках книги и папки с документами | |
| 3.3 | Сейф напольный | замок механический кодовый | |
| 3.4 | Стол приставной | имеет под столешницей полку | |
| 3.5 | Столик под телевизионную аппаратуру | 1 шт. | |
| 3.6 | Доска-экран | размер 2000 × 1200 мм, из белого пластика, на котором можно рисовать фломастером и использовать в качестве экрана | |
| 3.7 | Кресло кожаное вращающееся | 1 шт. | |
| 3.8 | Кожаные кресла для отдыха | 2 шт. | |
| 3.9 | Журнальный столик | 1 шт. | |
| 3.10 | Стол для заседаний | рассчитан на 10 человек | |
| 3.11 | Стулья | деревянные полужесткие, 10 шт. | |
| **4** | **Радиоэлектронные средства и электрические приборы** | | |
| | *а*) Основные | | |
| 4.1 | Компьютер | состав: системный блок, монитор, мышь, клавиатура, 2 динамика, на письменном столе | |
| 4.2 | Телефон закрытой связи (ЗАС) | на приставном столике | |
| 4.3 | Видеодвойка (телевизор + видеомагнитофон) | в случае просмотра видеокассет с закрытой информацией | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | *б*) Вспомогательные | | |
| 4.4 | Телефон городской АТС | на приставном столике | |
| 4.5 | Телефон внутренней АТС | на приставном столике | |
| 4.6 | Концентратор | под столешницей приставного столика | |
| 4.7 | Видеодвойка | просмотр видеокассет с открытой информацией | |
| 4.8 | Вентилятор | на письменном столе | |
| 4.9 | Вторичные часы единого времени | на стене, смежной с приемной | |
| 4.10 | Громкоговоритель оповещения | на стене, смежной с коридором | |
| 4.11 | Настольная лампа | 1 шт. | |
| 4.12 | Люстра из 5 рожков | на потолке | |
| 4.13 | Извещатели пожарные | 2 шт. на потолке | |
| **5** | **Средства коммуникаций** | | |
| 5.1 | Розетки электропитания | одна возле письменного стола, другая возле видеодвойки | |
| 5.2 | Телефонные розетки | 2 шт., возле письменного стола | |
| 5.3 | Электропроводка | скрытая в стенах | |
| 5.4 | Кабели телефонных линий | наружные, на стене возле письменного стола | |
| 5.5 | Кабель локальной сети ЭВМ | витая пара, укрепленная на стене | |
| 5.6 | Шлейф пожарной сигнализации | наружный, на потолке и стене возле письменного стола | |

*Примечание.* Характеристики ограждений, указанные в этой таблице, занижены по сравнению с типовыми реальными значениями с целью выявления большего количества угроз подслушивания.

## 2. Моделирование угроз информации в кабинете руководителя

Информация в кабинете подвергается угрозам воздействия и утечки. Эти потенциальные угрозы существуют всегда, но возможность их резко возрастает, когда злоумышленник пытается проникнуть в организацию или вербует сотрудника, возникает очаг пожара или проявляются достаточно информативные признаки технических каналов утечки информации.

### 2.1. Моделирование угроз воздействия на источники информации

При моделировании угроз воздействия прогнозируются маршруты движения злоумышленника из нулевого состояния вне территории организации к источникам информации в кабинете руководителя, оцениваются параметры (вероятность и время реализации) отдельных участков маршрутов (дуг семантической сети). По ним оценивается ущерб и ранг угроз.

Способы проникновения злоумышленника в кабинет руководителя зависят от квалификации злоумышленника, модели объектов защиты и времени проникновения.

В данном сценарии рассматривается вариант проникновения квалифицированного злоумышленника, который имеет в организации сообщника без специальной подготовки.

Время проникновения целесообразно разделить на рабочее и нерабочее. Рабочее время характеризуется следующими условиями: пропуск людей и автотранспорта производится через контрольно-пропускной пункт (КПП) по пропускам, извещатели технических средств охраны на территории и в здании выключаются, входная дверь в административное здание, в котором размещается кабинет руководителя, открывается для свободного прохода.

В рабочее время несанкционированное проникновение в организацию возможно через КПП по фальшивым документами и через забор. Хотя второй способ проникновения в рабочее время маловероятен, полностью исключить его нельзя. В рабочее время проникнуть в кабинет может как «чужой» злоумышленник, так и сотрудник организации. Очевидно, что сотруднику сделать это про-

ще. Проникновение возможно при открытых и закрытых дверях кабинета и приемной, но наиболее легкий вариант для злоумышленника — обе двери открыты. Такой вариант в принципе возможен, когда руководитель уходит или выходит из кабинета, а секретарь выходит из приемной, не закрыв оба кабинета. Более реален вариант — дверь кабинета закрыта, а в приемную открыта.

Во внерабочее время проникновение злоумышленника в организацию возможно через забор, а также через окно или дверь здания, примыкающего к тротуару.

Если злоумышленник имеет предварительную информацию о расположении и типах средств охраны и видеоконтроля, он может попытаться проникнуть в кабинет во внерабочее время путем скрытного преодоления в ночное время рубежей и зон безопасности или спрятавшись в конце рабочего дня в одном из незакрываемых помещений организации. Возможные варианты проникновения злоумышленника в кабинет представлены в виде семантической цепи, обозначения которой соответствуют обозначениям на рис. П.1.3.

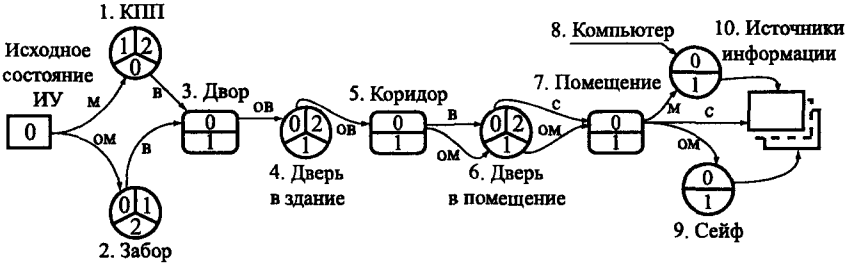



*Рис. П.1.3.* Графическая модель проникновения злоумышленника к источникам информации в кабинете руководителя в рабочее время

*Примечание.* Градации вероятностей перехода: ом — очень малая, м — малая, с — средняя, в — высокая, ов — очень высокая.

## 2.2. Моделирование технических каналов утечки информации

Моделирование выявленных технических каналов утечки информации предполагает определение показателей их угроз.

### *2.2.1. Моделирование оптических каналов утечки информации*

Возможны следующие оптические каналы утечки информации из кабинета руководителя:

- объект наблюдения в кабинете — окно кабинета — окно противоположного дома — оптический прибор злоумышленника;
- объект наблюдения в кабинете — приоткрытая дверь — злоумышленник;
- объект наблюдения в кабинете — телевизионное закладное устройство — проводной или радиоканал — телевизионный приемник злоумышленника.

Вероятность обнаружения объектов наблюдения в кабинете и их распознавания зависит от количества и информативности видовых демаскирующих признаков. Эти признаки добываются из изображения объекта наблюдения на сетчатке глаза, фотоснимке, фоточувствительной поверхности оптического приемника. Количество признаков зависит от:

- разрешающей способностью оптического приемника;
- масштаба изображения относительно реального объекта.

Минимальные размеры элемента изображения объекта наблюдения на светочувствительном элементе, наблюдаемого в виде точки, определяются как $\Delta h \approx D / Rf$, где D — дальность от светоприемника до объекта наблюдения, f — фокусное расстояние объектива оптического приемника.

В качестве технического средства наблюдения за объектами в кабинете через его окна рассматривается фотоаппарат ФС-122 («Фотоснайпер») с объективом Таир-30, фокусное расстояние которого равно 300 мм, а разрешающая способность объектива $R_o \approx 50$ лин/мм. Такой фотоаппарат размещается в удобном для скрытного переноса портфеле типа «кейс». При использовании фотопленки с разрешающей способностью $R_{фп} = 100$ лин/мм разрешение фотоаппарата (объектива — пленка) R = 33 лин/мм. Для D = 50 м размеры элемента объекта, отображаемого на светочувствительном элементе в виде точки-пикселя, соответствующего $\Delta h \approx 10$ мм. Минимальные линейные размеры объекта, который можно распознать с вероятностью 0,9, составляют 5–6 см.

Такие минимальные размеры могут иметь буквы и цифры на плакатах, иллюстрирующих выступления докладчиков на ответственных совещаниях. При полученных значениях разрешения могут быть также распознаны лица людей и внешний вид достаточно крупной продукции. Однако прочитать текст на документах формата А4, рассмотреть изображение на экране компьютера и телевизора, прочитать произносимые слова по губам нельзя. Следовательно, риск рассмотренного оптического канала утечки информации, содержащейся в изображении плакатов, людей и крупногабаритной продукции велик, а утечки информации в изображениях документов размера А4 и продукции малого размера очень мал.

Другой оптический канал утечки информации может возникнуть при приоткрытой двери кабинета или при заглядывании в кабинет посторонних лиц. В этом случае могут быть прочитаны тексты не только на плакатах, но и на столах и на экранах светопроектора и телевизора. Но при наличии бдительного секретаря в приемной возможность такого наблюдения очень мала.

Наконец, возможность реализации угрозы наблюдения с помощью видео закладного устройства также мала, так как установка телевизионной камеры в кабинете — серьезная разведывательная операция. Однако пренебрегать такой возможностью нельзя.

На основании этих результатов риск утечки информации при наблюдении можно оценить следующим образом:

- семантической документальной информации, отображаемой на плакатах — очень высокий, остальной документальной информации — очень малый;
- о видовых признаках людей — средний;
- о видовых признаках продукции — малый;
- о видовых признаках веществ и материалов — очень малый.

### *2.2.2. Моделирование акустических каналов утечки информации*

Утечка речевой информации возможна по следующим прямым (без ретранслятора) акустическим техническим каналам:

- источник речевого сигнала — стена в соседнее помещение — акустический приемник злоумышленника;
- источник речевого сигнала — приоткрытая дверь в приемную — акустический приемник;

- источник акустического сигнала — закладное устройство — радиоканал — радиоприемник злоумышленника;
- источник акустического сигнала — стекло окна — модулированный лазерный луч — фотоприемник лазерной системы подслушивания;
- источник акустического сигнала — воздухопровод — акустический приемник;
- источник акустического сигнала — случайный акустоэлектрический преобразователь в техническом средстве — побочное излучение технического средства — радиоприемник;
- источник акустического сигнала — случайный акустоэлектрический преобразователь в техническом средстве — проводные кабели, выходящие за пределы контролируемой зоны;
- источник акустического сигнала — воздушная среда помещения — диктофон у злоумышленника.

Для оценки угроз речевой информации необходимо оценить уровень акустического сигнала в возможных местах размещения акустического приемника злоумышленника. Такими местами являются:

- приемная;
- коридор
- смежные с кабинетом помещения;
- помещения с трубами отопления, проходящими через кабинет;
- помещения, акустически связанные с кабинетом через воздуховоды вентиляции.

Кроме того, речевая информация в кабинете может ретранслироваться по радиоканалу или проводам телефонной линии и электропитания закладными устройствами и побочными электромагнитными излучениями основных и вспомогательных технических средств и систем, а также средствами лазерного подслушивания. Так как носителями информации при ретрансляции являются электромагнитная волна в радиодиапазоне и электрический ток, то угрозы и меры по предотвращению перехвата рассматриваются в радиоэлектронном канале утечки информации. Также в принципе акустическая информации может быть добыта с помощью лазерного средства подслушивания, установленного в помещении противоположного дома.

В качестве критерия защищенности речевой информации используется отношение сигнал/шум, при котором качество подслушиваемой речевой информации ниже допустимого уровня. В соответствии с существующими нормами понимание речи невозможно, если отношение помеха/сигнал равно 6–8, а акустический сигнал не воспринимается человеком как речевой, если отношение помеха/сигнал превышает 8–10. Следовательно, для гарантированной защищенности речевой информации отношение сигнал/шум должно быть не более 0,1 или (–10) дБ. Оценка угрозы акустического канала утечки информации при подслушивании человеком производится по формуле: $L_п = L_и - Q_{ог} - L_ш$. При применении технического акустического приемника эта величина увеличивается на 6 дБ.

Значения входящих в формулу слагаемых указаны в справочниках по акустике, отдельные в табл. П.1.3.

*Таблица П.1.3*

| *Характеристика речи* | *Громкость, дБ* | *Основной элемент среды распространения* | *Величина звукоизоляции, дБ* | *Место нахождение акустического приемника* | *Уровень шума, дБ* |
|---|---|---|---|---|---|
| Спокойный разговор | 50–60 | Стена и дверь в приемную | 27 | Приемная | ~30 |
| Громкая речь | 60–70 | Стена в коридор | 51 | Коридор | 35–40 |
| Шумное совещание | 70–80 | Стена в смежную комнату | 40 | Соседнее помещение | 20–25 |
| | | Межэтажное перекрытие | 50 | Помещения на верхнем и нижнем этажах | 25–30 |
| | | Вентиляционный короб | 0,2 дБ/м 3–7дБ на изгиб | В вентиляционной отверстии другого помещения | 30 |
| | | Трубы отопления | 25–35 | На трубе отопления | 30 |

Уровни громкости речевой информации в возможных местах размещения акустического приемника злоумышленника при громкости источника 70 дБ указаны в табл. П.1.4.

*Таблица П.1.4*

| *№ п/п* | *Место размещения акустического приемника злоумышленника* | *Уровень громкости* | *Риск подслушивания* |
|---|---|---|---|
| 1 | Приемная | 5–10 | Очень высокий |
| 2 | Коридор | –15–(–20) | Отсутствует |
| 3 | Соседнее помещение | ~ (–5) | Низкий |
| 4 | Верхнее (нижнее) помещение | –5–(–10) | Отсутствует |
| 5 | Вентиляционный короб | 0–5 | Средний |
| 6 | Трубы отопления | 0–5 | Средний |

Как следует из данных табл. П.1.4 наибольшую угрозу создает канал утечки, приемник которого расположен в приемной и в коробе вентиляции. Каналом утечки, приемник которого расположен в коридоре, можно пренебречь.

### *2.2.3. Моделирование радиоэлектронных каналов утечки информации*

Радиоэлектронные каналы утечки информации из кабинета руководителя кабинета представляют собой простые каналы и части составных акусто-радиоэлектронных каналов утечки информации. Простые каналы образованы побочными электромагнитными излучениями и наводками радиосредств и электрических приборов, размещенных в кабинете, в том числе:

- компьютера при обработке на нем закрытой информации;
- видеодвойки (в случае просмотра видеокассет с закрытой информацией).

Кроме того, опасные сигналы случайных акустоэлектрических преобразователей в радиосредствах и электрических приборах могут добавить к простым оптическим и акустическим каналам радиоэлектронные каналы утечки информации и создать составные акусто-радиоэлектронные и оптико-радиоэлектронные каналы утечки. Источниками радиоэлектронных каналов утечки в составе акусто-радиоэлектронных составных являются:

- коммутационное оборудование и кабели внутренней АТС;
- электрические приборы в кабинете (вторичные часы единого времени, вентилятор, громкоговоритель оперативного оповещения);
- передатчики акустических и телевизионных закладных устройств.

Если в кабинете установлено телевизионное закладное устройство, например, в типовых папках (скоросшивателях) с отверстием в торце, то составной оптико-электронный канал утечки информации содержит радиоэлектронный канал утечки с элементами: телевизионная камера — телевизионный приемник — видеомагнитофон или злоумышленник наблюдатель.

Побочные НЧ и ВЧ излучения ОТСС имеют очень широкий диапазон частот — доли Гц–тысячи МГц (длины волн — сотни метров—десятки сантиметров). Помещение кабинета, учитывая его размеры, представляет собой ближнюю, переходную и дальнюю зону побочного излучения ОТСС. На частотах до 30 МГц помещение образуют ближнюю зону. В зависимости от вида излучателя в ближней зоне может преобладать электрическое или магнитное поля.

Информация в помещении находится в безопасности, если уровни ее носителей в виде электрических сигналов и напряженности поля не превышают нормативы. Следовательно, для предотвращения подслушивания путем перехвата опасных сигналов необходимо определить эти уровни на границе контролируемой зоны (периметра кабинета) и в случае недопустимо больших значений определить рациональные меры их по уменьшению.

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, соизмеримая с размерами ячейками арматуры.

При ослаблении электромагнитной волны стенами здания на 20 дБ дальность ее распространения уменьшается на 1 порядок. Для рассмотренного примера она составит единицы сотен и десят-

ки метров. Учитывая, что окна кабинета выходят на улицу, риск перехвата радиоизлучений ПЭВМ из кабинета руководителя организации можно оценить значением «средний», а электрических сигналов акустоэлектрических преобразователей — «низкий».

Таким образом, наибольший ущерб информации, содержащейся в кабинете руководителя, могут нанести следующие угрозы:

- наблюдение из окна противоположного дома текста и изображений на плакатах экранах, укрепленных на стенах кабинета;
- подслушивание разговора в кабинете через приоткрытую дверь в приемную руководителя;
- подслушивание громкого разговора через стену, разделяющую кабинет и коридор;
- наблюдение через окно противоположного дома за участниками совещания;
- наблюдение через приоткрытую дверь за участниками совещания;
- перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;
- перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, трансляции, часов единого времени, электропитания и заземления;
- подслушивание с помощью стетоскопа речевой информации акустических сигналов, распространяющихся по трубам отопления;
- подслушивание речевой информации акустических сигналов, распространяющихся по воздухопроводам;
- подслушивание с помощью акустических закладных устройств, установленных в кабинете;
- скрытое наблюдение с помощью предварительно установленных телевизионных камер;
- скрытное проникновение к источникам информации, хранящихся в ящиках стола, в компьютере, в сейфе.

## 3. Нейтрализация угроз информации в кабинете руководителя организации

### 3.1. Меры по предотвращению проникновения злоумышленника к источникам информаци

Так как проникновение злоумышленника возможно через дверь в приемную, то в ночное время необходимо создать дополнительный рубеж и контролируемую зону в приемной Для этого на двери из коридора в приемную устанавливается магнитоконтактный извещатель типа СМК-3 или более современные ИО-104-2, 4. Датчик ИО-104-4 имеет меньшие габариты. Эти извещатели обеспечивают замыкание и размыкание контактов геркона при приближении магнита к геркону на расстояние не более 10 мм контакты и удалении более 45 мм.

Аналогичный извещатель устанавливается на дверях кабинета. Для обнаружения злоумышленника в кабинете необходимо установить объемный извещатель. В кабинете в принципе можно установить пассивный оптикоэлектронный, ультразвуковой, радиоволновый и комбинированный извещатели. Выбор производится по помехоустойчивости, объему кабинета и затрат на приобретение и эксплуатацию. В отличие от приемной, средства охраны которой в рабочее время отключаются, средства охраны кабинета при отсутствии на рабочем месте руководителя организации целесообразно сохранять во включенном состоянии. Для обеспечении такого режима необходимо использовать отдельный шлейф.

Учитывая небольшую площадь кабинета, целесообразно применять или пассивные оптико-электронные извещатели или активные волновые с регулируемой мощностью излучения. В качестве таких средств могут использоваться оптико-электронный извещатель «Фотон-5», создающий «занавес» с максимальной дальностью 12 м, ультразвуковой «Эхо-2» для площади 30 м$^2$, радиоволновой объемный «Волна-5» с регулируемой дальностью 2–16 м и комбинированный извещатель «Сокол-2», совмещающий пассивный инфракрасный и радиоволновой принципы обнаружения. Последний обеспечивает дальность действия: минимальную — 3–5 м, максимальную — 12 м. Он может крепиться к стене или на потолке, имеет высокую помехоустойчивость. Из сравнительного анализа ука-

занных извещателей можно сделать вывод о том, что наиболее дешевым извещателем с приблизительно равными функциональными возможностями является оптико-электронный извещатель «Фотон-5». По критерию эффективность/стоимость лучшие показатели имеет комбинированный извещатель «Сокол-2».

Кроме рассмотренных средств целесообразно установить локальные извещатели для охраны сейфа и компьютера. Для охраны сейфа можно использовать охранный поверхностный емкостной извещатель «Пик» с регулируемой чувствительностью на приближение человека в интервале до 0,2 м.

Для защиты информации в компьютере от физического контакта его с злоумышленником и хищения информации путем копирования или изъятия винчестера качестве извещателя можно использовать также емкостной извещатель «Пик», антенна которого соединена с корпусом сейфа. Для механической защиты системный блок с винчестером может быть размещен в специальном сейфе под приставным столиком или использоваться съемный винчестер, помещаемый в сейф.

### 3.2. Защита информации в кабинете руководителя от наблюдения

Для защиты информации от наблюдения применяют методы энергетического скрытия путем увеличения затухания среды распространения. Для прекращения функционирования оптического канала утечки информации «окно кабинета — окно противоположного жилого дома» можно применить следующие меры:

- шторы на окна;
- жалюзи;
- тонированные пленки на стеклах.

Шторы — традиционные средства для предотвращения скрытного наблюдения через окна кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете, незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты делать не сле-

дует. Для обеспечения скрытности защиты применять пленку надо на всех окнах, по крайней мере, этажа, а лучше здания.

Наиболее приемлемый вариант защиты — применение жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению — защите от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

Меры по обнаружению и локализации скрытно установленной в кабинете телевизионной камеры проводятся периодически и перед проведением совещания. Исключить установку камеры между проверками нельзя. Телевизионное изображение может передаваться в реальном масштабе времени или записываться на пленочный или цифровой видеомагнитофон с последующей ускоренной передачей. Однако, учитывая, что кинематический видеомагнитофон имеет большие, чем телевизионная камера, размеры и энергопотребление, его практическое применение в настоящее время ограничено. В будущем следует ожидать появление бескинематических цифровых видеомагнитофонов для скрытой записи. Основным демаскирующим признаком телевизионной камеры и видеомагнитофона является радиоизлучение. Поэтому для обнаружения и локализации телевизионной камеры применяются средства поиска радиоизлучающих закладных устройств: индикаторы поля, специальные радиоприемники, автоматизированные комплексы для радиомониторинга и др. Перед совещанием во время «чистки» кабинета применяются также нелинейные локаторы и металлодетекторы.

### 3.3. Меры по защите речевой информации от подслушивания

1. Для защиты от подслушивания речевой информации в приемной необходимо существенно повысить звукоизоляцию дверей как наиболее слабого звена в акустической защите и стены до, по крайней мере, до 55 дБ на частоте 1000 Гц. Такая звукоизоляция обеспечивается двойной дверью с тамбуром шириной не менее 20 см с уплотнителями по периметру дверных полотен. Для предотвращения утечки информации через ограждения кабинета возможны 3 варианта:

- повышение поверхностной плотности ограждения;
- установление дополнительной перегородки;
- зашумление ограждения.

Так как звукоизоляция пропорциональна поверхностной плотности среды распространения акустической волны, то при недостаточной звукоизоляции утолщают стены. Наиболее удобным строительным материалом для этого является кирпич, который укладывают на ширину половины или длины целого кирпича вплотную к стенке.

Возможно также укрепление на стене строительных материалов (многослойной фанеры различной толщины, стеклопластика, пемзобетонных плит и др.).

Утолщенная стена из красного кирпича обеспечивает повышение звукоизоляции с 48 дБ до 53 дБ. Кладка утолщенной стены с зазором между стенками 40 мм увеличивает звукоизоляцию еще приблизительно на 4–5 дБ. Утолщение стены целесообразно проводить со стороны приемной, так как это позволит уменьшить выступ двойной двери с тамбуром в приемную.

Звукоизоляция стен между кабинетом и приемной, кабинетом и коридором, кабинетом и смежным помещением повышается путем утолщения стен и крепления к ним дополнительных перегородок. Утолщение стен производится путем кирпичной кладки у стены кабинета. В качестве дополнительных перегородок используются асбестоцементные, гипсокартонные, древесностружечные, древесноволокнистые плиты толщиной 10–20 мм. Они крепятся к стене с помощью деревянных реек и брусков толщиной 40–50 мм по периметру и поверхности стены. По периметру между перегородкой и другими ограждениями устанавливаются упругие (из губчатой резины) прокладки. Между перегородкой и стеной может быть размещен звукопоглощающий пористый материал.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете, на стенах могут быть укреплены виброакустические излучатели акустических генераторов помех.

Для исключения утечки информации через батареи и трубы отопления перед батареями устанавливают резонаторные экраны в виде деревянных перегородок с отверстиями.

Для предотвращения утечки информации через вентиляционное отверстие пред ним укрепляют экран и (или) размещают в нем глушитель звука.

С учетом рассмотренного в качестве мер предотвращения подслушивания рекомендуется:

- установка двойной двери с уплотнительными прокладками и тамбуром глубиной 30 см;
- увеличение толщины стены между кабинетом и приемной, а также соседними помещениями на 0,5 кирпича;
- установка на батареи отопления резонаторных экранов или излучателей генератора виброакустического зашумления;
- закрытие окна плотными шторами, установка на стекла окон излучателей генератора виброакустического зашумления (для предотвращения лазерного подслушивания при закрытых окнах);
- установка перед воздухозаборниками воздухопроводов акустических экранов;
- установка датчиков комплекса обнаружения скрытно работающего диктофона PDTR-18 под столешницу стола руководителя возле стула для посетителя и стола заседания;
- применение устройств для подавления сигналов скрытно работающего диктофона.

Установка двойной двери повышает звукоизоляцию с 18 дБ до 48 дБ, утолщение стены увеличивает звукоизоляцию примерно на 20 дБ.

### 3.4. Предотвращение перехвата радио- и электрических сигналов

Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается:

- выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись;
- установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания;
- установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» и «Гранит-VIII» — ограничителей малых амплитуд с фильтрами от ВЧ-навязывания;

- установкой НЧ-фильтров в цепь вторичных часов единого времени (устройство МП-4);
- установкой буфера в цепь громкоговорителя системы оповещения (устройство МП-5);
- использованием в кабинете генератора пространственного электромагнитного зашумления кабинета, включаемого во время проведения совещения с по тематике, содержащей тайну;
- установкой в свободный слот системной платы компьютера платы генератора помех.

Кроме того, информация на компьютере в кабинете руководителя организации может защнщаться путем:

- использования защищенных ПЭВМ;
- размещения системного блока в специальном сейфе;
- установкой винчестера в съемный кожух и хранение его в сейфе;
- программной защиты доступа к компьютеру и отдельным папкам;
- криптографическим шифрованнем информации, хранящейся на машинных носителях.

Кроме того, после проведения капитального ремонта и перед проведением совещания производится чистка помещения с целью обнаружения закладных устройств.

*Приложение 2*

# Технические средства добывания информации

## 1. Технические средства наблюдения

*Таблица П.2.1*

| *Наименование средства, производитель* | *Функциональные и технические характеристики* | *Габариты, масса* | *Примечание* |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Устройство передачи видео и аудио информации **«Пачка»**, SET-1, Россия | Частота сигнала — 950–1200 МГц, мощность — 50 мВт, дальность работы в помещении — 15–30 м, разрешение — 380 твл, чувствительность — 2–3 лк, угол зрения — 40–70° | | Может быть установлено в пачке сигарет |
| Устройство передачи аудио и видеоинформации **«Сотовый телефон»**, SET-1, Россия | То же, чувствительность — 380 твл (цвет.), 420 твл (ч/б) | В корпусе сотового телефона | |
| Скрыто носимый комплект для передачи аудио- и видеоинформации **«Пояс»**, SET-1, Россия | Частота сигнала — 950–1200, 270–310 МГц, мощность — 700 мВт, средняя дальность в помещении — 30–50 м, в открытом помещении — 300–500 м | Установлен в тканевом поясе | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Фотоаппарат **«Зенит-МА-2»**, ОАО «Красногорский завод», Россия | Фокусное расстояние объектива — 24 мм, формат кадра — 14,8 × 21 мм, емкость кассеты — 30 кадров, диапазон выдержек — 1/60–1/1000 с, покадровая и непрерывная съемка | 29 × 65 × 96 мм, 230 г | |
| Фотоаппарат **«Зенит-МФ-1»**, ОАО «Красногорский завод», Россия | Фокусное расстояние объектива — 28 мм, размер кадра — 18 × 24 мм, емкость кассеты — 14 кадров, привод — пружинный | 77,2 × 40,5 × 55 мм, 180 г | |
| Бинокулярный прибор **БС 16 × 40**, ОАО «Красногорский завод», Россия | Увеличение — 16 крат, угол зрения — 3°, стабилизация изображения | 240 × 190 × 100 мм, 2 кг | |
| Телевизионная система ночного видения **«СИЛИНК»**, ООО «ТУРН», Россия | Поле зрения — 6° × 4,8°, дистанция обнаружения человека — 500–900 м ($10^{-2}$–$10^{-3}$ лк), точность определения координат — 25 м, разрешение — 450 твл | 190 × 430 × 370 мм, 15 кг — оптический блок; 230 × 250 × 220, 6 кг — монитор | |
| Специальная фотокамера **РК 420** | Размер кадра — ∅ 5,5 мм, число кадров — 7 | Часы: ∅ 34 мм, толщина — 7 мм, 70 г | Вмонтирована в электронные часы |
| **Прибор дальнего наблюдения и фотографирования**, ОАО «Красногорский завод», Россия | Увеличение — 13,7–41 крат, фокусное расстояние объектива — 700–21000 мм, угол зрения, град. — 3,5–1,06, размер кадра — 24 × 36 мм. | 480 × 400 × 790 мм, 58 кг | |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| Прибор ночного видения **«Night Master NS-2033»** | Увеличение — до 3 крат, угол зрения, град. — 40–12, разрешение в центре — 36 лин/мм, усиление — 25000 | 105 × 48 × 68 мм, 0,425 кг | |
| Ночной оптический локатор **«TITAN-720»** | Дальность распознавания — до 1000 м, точность измерения расстояния — 10 м, увеличение — 2, 5 крат, коэффициент усилеиия — 50000 | 330 × 170 × 85 мм, 2,2 кг | |
| Прибор ночного видения **EEV Nite-Watch Plus,** EEV, Великобритания | Усиление яркости — 20000, продолжительность непрерывной работы от одной батареи — 3 ч | ∅ 46 × 120 мм, 330 г | Комплексируется с фото- и видеокамерами |
| Телевизионная камера **WAT-660D-P3, 7,** Watec, Япония | Мин. освещенность — 4 лк, разрешение — 380 твл, фокусное расстояние объектива — 4,5 см, угол зрения — 59° | 30 × 30 × 16 мм | Бескорпусная с вынесенным объективом |
| Специальный эндоскоп **PK1700** | Длина — 170 мм, диаметр объектива — 1,7 мм, угол зрения — 70°, подсветка специальным источником мощностью 150 Вт | | Для чтения текста в запечатанном конверте |

## 2. Технические средства подслушивания

*Таблица П.2.2*

| *Наименование средства, производитель* | *Функциональные и технические характеристики* | *Габариты, масса* | *Примечание* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| Направленный микрофон **НМ 011 «Кейс»**, SET-1, Россия | Дальность контроля информации (при разборчивости 50%) — 10 м, время непрерывной записи — 90–120 мин | 105 × 405 × 445 мм | |
| **Параболический микрофон** | Диапазон частот — 150–20000 Гц, акустическое зеркало диаметром 47,6 см, дальность | 1,2 кг | |
| Радиомикрофон **РМК 153 «Тройник»**, SET-1, Россия | Частота излучения — 416,5–423,3 МГц, кварцевая стабилизация, вид модуляции — WFM, $P_{вых}$ — 7 мВт, дальность передачи — 150 м | | Установлен в сетевой тройник |
| Радиомикрофон **РМК 081 «Ручка»**, SET-1, Россия | Частота излучения — 416,5–423,3 МГц, кварцевая стабилизация, вид модуляции — WFM, $P_{вых}$ — 7 мВт, дальность передачи — 100 м, время непрерывной работы — 6 ч | | Установлен в ручке |
| Сетевой удлинитель **«Сеть 2Ч»** | Передача информации по электросети, ЧМ, дальность — 200 м. | | |
| Диктофон цифровой **«Спутник-SM»** | Макс. время записи — 37,3 ч (флэш-память 512 Мб), чувствительность — 7–9 м, голосовая активация | 45 × 25 × 7 мм (для варианта камуфляжа в брелке) | |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| Устройство долговременной звукозаписи **«Слог-02»** | Время непрерывной записи — 12 ч (МК-120), автореверс | | Встроен в радиоплеер RQ-A171 фирмы Panasonic |
| Микрокассетный диктофон **«Olympus L-400»** | Время записи — 4 ч (С-120), активация голосом, автореверс, полное дистанционное управление | 73 × 52 × 20 мм, 90 г. | |
| Электронный стетоскоп **РК-845-SS**, PK Electronik | Тип микрофона — электретный, толщина стены — до 0,7 м, коэффициент усиления — 25000, длина провода — до 500 чм | 440 × 320 × 100 мм, 3,9 кг — усилительный блок | |
| Средство лазерного подслушивания **РК-1035-SS**, PK Electronik | Длина волны полупроводникового лазера — 0,85 мкм, мощность излучения — 5 мВт | Пер-к: 250 × ∅ 65 мм, 1,6 кг; пер-к: 260 × ∅ 65 мм, 1,5 кг; электр. блок: 460 × 330 × 120 мм, 3,2 кг | |

## 3. Технические средства перехвата сигналов

*Таблица П.2.3*

| *Наименование средства, производитель* | *Функциональные и технические характеристики* | *Габариты, масса* |
|---|---|---|
| *1* | *2* | *3* |
| Семейство носимых многофункциональных комплексов радиомониторинга и пеленгования **АРК-НК**, ЗАО «Иркос» | Рабочий диапазон в максимальной конфигурации — 9 кГц–18 ГГц, скорость поиска — 100 МГц/с, чувствительность — 1–2 мкВ, инструментальная точность пеленгования — 10–20° (при скрытом), 7–15° (ручном), 5–7° (автоматическом), скорость переключения каналов — 30 кан/с, длительность непрерывной записи в ЗУ — 1 ч | Унифицированные по габаритам модули, допускающие размещение в папке, в разгрузочном жилете, в сумке для видеокамеры, в рюкзачке, на посту оператора |
| Комплекс контроля радиотелефонных каналов **АРК-РД6**, ЗАО «Иркос» | Количество контролируемых каналов — 6, рабочий диапазон частот — 25–1300 МГц, полоса анализа — 4 МГц, количество частот в задании — 255 | Стойка с 6 приемниками, блок аналого-цифровой обработки, ПЭВМ, комплект кабелей |
| Аппаратура перехвата каналов общего применения **«Родея-М»**, фирма «Радэп» | Диапазон частот Гц, ширина одновременной обработки сигналов — 10 МГц, время обработки — 50 мс | |
| Комплекс перехвата пейджинговых сообщений **4630-PAG-INT** | Диапазон частот — 25 МГц–2 ГГц, виды модуляции — AM, FM, SSB, чувствительность в режиме FM — 0,5 мкВ, избирательность — 7,5 кГц (AM, FM), 1,4 кГц (SSB) | |

| *1* | *2* | *3* |
|---|---|---|
| Комплекс перехвата факсимильных передач **4605-FAX-INT** | Контроль до 4 проводных факсов, автоматическое распознавание речевых и факсимильных сообщений, регистрация до 4000 страниц факсимильных сообщений | |
| Комплекс перехвата информации, обрабатываемой на ЭВМ, **4625-COM-INT** | Диапазон частот — 25 МГц–2 ГГц, предельная чувствительность — 0,15 мкВ, диапазон частот развертки — 14–38 кГц (строчная), 40–120 Гц (кадровая) | 25 × 55 × 35 см, 18 кг |
| Анализатор спектра **HP 8564E**, Hewlett Packard | Диапазон частот — 9 кГц–40 ГГц, чувствительность — (–145) дБ, погрешность измерения — 3 дБ (амплитуды), 1 кГц (частоты), тип детектора — AM, FM | 325 × 163 × 427 мм, 20 кг |
| Анализатор спектра **ESS**, «Rohde&Schwarz» | Диапазон частот — 5 Гц–1000 МГц, предельная чувствительность — 0,25 мкВ (F = 10 кГц), тип детектора — AM, FM, LSB, USB, погрешность измерения — 1–2 дБ (амплитуды), 10 Гц (частоты до 30 МГц), 100 Гц (более 30 МГц) | 435 × 236 × 363 мм, 37 кг |
| Сканирующий радиоприемник **AR-5000**, AOR | Диапазон частот — 10 кГц — 2600 МГц, виды модуляции — AM, FM, LSB, USB, CW, предельная чувствительность — 0,36–0,56 мкВ (AM), 0,2–1,25 мкВ (FM), 0,14–0,25 мкВ (LSB, USB), избирательность — 3, 6, 15, 40, 110, 220 кГц, шаг перестройки — от 1 Гц до 1 МГц, число каналов памяти — 1000, скорость сканирования — 50 канал/с | 204 × 77 × 240 мм |
| Комплекс для съема информации с кабельных линий **«Крот»** | Съем информации с помощью индукционного датчика-захвата, одновременная запись по 60 телефонным каналам, продолжительность непрерывной записи — 115 ч, оборудован радиомаяком | |

*Приложение 3*

# Технические средства инженерно-технической защиты информации

## 1. Извещатели контактные

*Таблица П.3.1*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса* | *Примечание* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| **АЛ-1-Т-0,02х10 «Фольга», «Фольга-С»** | «Фольга»: ширина — 6–12 мм, толщина — 0,008–0,04 мм; «Фольга-С»: самоклеющаяся, ширина — 10 мм, толщина — 0,014 мм, длина рулона — 5–20 м | | «Фольга» приклеивается клеем «Контакт», краской, грунтовкой и др. |
| Конечные выключатели **ВК-200, ВК-300** | Величина коммутируемого напряжения, В — 380 (переменного), 220 (постоянного), коммутируемый ток — 0,05 А (минимальный), 6 А (номинальный) | 121 × 66 × 60 мм | |
| Магнитоконтактные извещатели **СМК-1, СМК-3, ИО 102-4, 5, 6** | Расстояние между геркоиом и магнитом: для замыкания контактов — 8–10 мм, для размыкания — 30–45 мм | 60 × 11 × 12, ∅ 8 × 21, 58 × 11 × 11, 31 × 13 × 6,5, ∅ 10 × 27, ∅ 23,5 × 37,5 мм | |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| Ударно-контактные **«Окно-2М, 4, 5, 6»** | Блокнруемая площадь обычного стекла — 4,5 м² (одним ДРС), 20 м² (комплектом), дальность ДРС — 2,5 м | ДРС: 35 × 9 × 8 мм, 80 г (О-4); 31 × 9,5 × 8,5 мм, 6 г (О-5); 31 × 9,4 × 8,4 мм, 6 г (О-6) | ДРС — датчик разрушения стекла |
| Пьезоэлектрические извещатели **5115, 5129**, Sentrol, Inc., США | Максимальная дальность действия — 2 м | 3,2 × 32 × 12 мм | |
| Извещатели обрывные **«Риф-ПД»**, **«Гамак»**, ПО «Старт» | Длина зоны обнаружения — до 1500 м («Риф-ПД»), до 500 м («Гамак») | | |
| Извещатель обрывной **«Кувшинка»**, НПО «Техника» МВД РФ | Длина зоны обнаружения — до 500 м, потребляемая мощность — 10 мВт | | |

## 2. Извещатели акустические

*Таблица П.3.2*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|
| Извещатели пьезоэлектрические **ИО 311-1 «Гюрза-050»**, **ИО 304-5 «Гюрза-050М»** | Масса охраняемого предмета: 0,05–20 кг («Гюрза-050»), 0,05–60 кг («Гюрза-050М»), чувствительность — 1 г | БОС «Гюрза-50»:148 × 110 × 40 мм, 0,6 кг; БОС «Гюрза-050М»: 205 × 110 × 42, 0,7 кг |
| Извещатели пьезоэлектрические **ИО 304-3 «Грань-2»**, **ИО 313-1 «Шорох-1»** | Максимальная охраняемая площадь: 8–15 м$^2$ («Грань-2»), 3–12 м$^2$ («Шорох-1») | БОС «Грань-2»: 190 × 155 × 45 мм, БОС «Шорох-1»: 123 × 57 × 26 мм |
| Звуковые извещатели **ИО 329-1 «Стекло-1»**, **ИО 329-2 «Стекло-2»**, **ИО 329-2А «Стекло-2-1»**, **ИО 329-4 «Стекло-3»** | Максимальная дальность действия — 6 м, контролируемая толщина стекла — 2,5–8 мм, максимальная контролируемая площадь стекла — 50 м$^2$ | «Стекло-1»: 100 × 90 × 40 мм, 0,25 кг; «Стекло-2»: 100 × 85 × 35 мм, 0,2 кг; «Стекло-2-1, 3»: 80 × 80 × 35 мм, 100 г |
| Извещатели ультразвуковые **ИОП 308-3 «Эхо-2»**, **ИОП 308-1 «Эхо-3»** | Макс. контролируемая площадь — 30–60 м$^2$, диапазон регулировки дальности — до 8 м, диапазон скорости злоумышленника — 0,3–2 м/с | «Эхо-2»: 245 × 175 × 163 мм, 1,4 кг (БОС); «Эхо-3»: 205 × 130 × 50 мм, 1,0 кг |
| Извещатель ультразвуковой **«Эхо-А»** | Контролируемая площадь — 25 м$^2$, дальность действия — 8,5 м | 227 × 63 × 50 мм, 350 г |
| Извещатель ультразвуковой **«Витрина»** | Контролируемый объем — 0,03–1,0 м$^3$, диапазон скорости злоумышленника — 0,02–1,0 м/с | 26 × 58 × 123 мм (БОС), 300 г |

*Примечание.* БОС — блок обработки сигналов.

## 3. Извещатели оптико-электронные

*Таблица П.3.3*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|
| **ИО 209-1 «Вектор-2», ИОП 209-4 «Вектор-3», ИО 209-13 «Вектор-СПЭК»** | Макс. дальность действия — 20, 100 м («В-2»); 0,5–10 м («В-3»); 75, 150 м («В-С»), мин. время перекрытия — 0,05–0,2 с, скорость пересечения — 0,1–3 м/с | «В-2»: 100 × 100 × 110 мм, 0,8 кг; «В-3»:160 × 115 × 63 мм, 0,8 кг; 75 × 95 × 145 мм, 1 кг |
| **ИО 209-4 «Рубеж-3М»** | Макс. дальность — 300, 600 м, макс. скорость пересечения луча — 5 м/с | 370 × 240 × 125 мм, 4 кг — БПК, 275 × 190 × 120 мм, 2,3 кг — БИ, БП |
| **ИО 409-2 «Фотон-6», ИО 409-5 «Фотон-8», ИО 409-8 «Фотон-9», ИО 409-6 «Фотон-СК», ИО 409-4 «Астра-МС»** | Тип зоны обнаружения — объемная, кол. чувствительных зон — 15 (Ф-6, 8), 35 (Ф-9), 33 (Ф-СК), 20 (А-МС), макс. дальность — 12 м (Ф-6,8), 10 м (Ф-9, СК), 12 м (А-МС) | Ф-6: 106 × 106 × 63 мм, 0,25 кг; Ф-8: 107 × 107 × 63 мм, 0,25 кг; Ф-9: 88 × 61 × 41 мм, 0,09 кг; Ф-СК: 68 × 127 × 48 мм, 0,09 кг; «А-МС»: 80 × 60 × 50 мм, 0,08 кг |
| **ИО 209-8 «Фотон-6А», ИО 209-13 «Фотон-8А»** | Тип зоны обнаружения — линейная, кол. чувствительных зон — 10, макс. дальность — 20 м, угол обзора в вертикальной плоскости — 45°, горизонтальной — 5° | Ф-6А: 106 × 106 × 63 мм, 0,25 кг; Ф-8А: 107 × 107 × 63 мм, 0, 25 кг |
| **ИО 309-2 «Фотон-6Б», ИО 309-6 «Фотон-6Б»** | Тип зоны обнаружения — поверхностная, кол. чувствительных зон — 1, макс. дальность действия — 10 м, контролируемая площадь — 50 м$^2$ | 107 × 107 × 63 мм, 0,25 кг |

*Примечание.* БПК — блок питания и контроля, БИ и БП — блоки излучателя и приемника.

## 4. Извещатели радиоволновые

*Таблица П.3.4*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|
| **ИО 407-5/2 «Аргус-2», «Аргус-2М», «Аргус-3»** | А-2: контр. площадь — 90 м$^2$, дальность — 2–16 м, контр. объем — 200 м$^3$, ширина/высота зоны обнаружения — 6–8/3–4 м; А-3: площадь — 25 м$^2$, дальность — 2–7,5 м, объем — 40 м$^3$, ширина/высота зоны — 5–6 м, скорость объекта — 0,3–3 м/с | А-2: 100 × 90 × 65 мм, 250 г; А-3: 90 × 75 × 40, 100 г |
| **ИО 307-2 «Волна-5»** | Контр. площадь — 90 м$^2$, дальность — 2–15 м, контр. объем — 200 м$^3$, ширина/высота зоны обнаружения — 6/8 м, скорость перемещения объекта — 0,3–3 м/с | 100 × 90 × 65 м, 200 г |
| **ИО 407-11 «Тюльпан-3»** | Контр. площадь — 90 м$^2$, дальность — 1,5–17 м, контр. объем — 250 м$^3$, ширина/высота зоны — 6–8/3–4 м, скорость перемещения объекта — 0,3–3 м/с | 95 × 75 × 70 мм, 250 г |
| **ИО 207-4 «Радий-2»** | Тип зоны обнаружения — объемный барьер, дальность — 20–200 м, ширина зоны обнаружения — 1,5–3 м, скорость движения злоумышленника — 0,3–10 м | 270 × 220 × 50 мм (передатчик, приемник), 1,1; 1,2 кг |
| **«Фон-1М»** | Контр. площадь — 300 м$^2$, макс. дальность — 40 м, контр. объем — 1000 м$^3$, ширина зоны обнаружения — 10м, скорость движения злоумышленника — 0,2–5 м, высота установки — 3–7 м | 310 × 350 × 160 мм, 15 кг |
| **«Шторм-2»** | Контр. площадь — 400 м$^2$, макс. дальность — 50 м, контр. объем — 4000 м$^3$, ширина зоны обнаружения — 10 м, ширина зоны обнаружения — 10 м, скорость движения злоумышленника — 0,2–5 м, высота установки — 3–7 м | 300 × 350 × 125 мм, 16 кг |

## 5. Извещатели вибрационные

*Таблица П.3.5*

| *Тип извещателя, производитель* | *Основные функциональные и технические характеристики, состав* | *Параметры питания* |
|---|---|---|
| *1* | *2* | *3* |
| **«Дельфин»**, **«Дельфин-МП»**, ГУП «Дедал» | Защита сетчатых и решетчатых заграждений, размер зоны — 250 м, на прямых участках — до 500м, состав: 1 блок электронный, КЧЭ 2 × 250 м, комплект монтажных частей | 20–30 В, до 0,1 Вт |
| **«Дрозд»**, ГУП «Дедал» | Вибромагнитометрическое средство для оград любого типа, размер зоны — до 500 м, блок электронный, проводной чувствительный элемент П-274, комплект монтажных частей | 20–30 В, до 0, 15 Вт |
| **«Годограф»**, НИКИРЭТ | Чувствительный элемент — кабель с центральным спиральным электродом, для защиты оград, размер зоны — до 250 м, блок электронный, КЧЭ | 10–30 В, до 16 мА |
| **«Амулет»**, ГУП «Дедал» | Противоподкопное средство с заглублением КЧЭ на глубину 5–20 см, размер зоны — до 1000 м, блок электронный, КЧЭ до 1000 м | 20–30 В, до 0,2 Вт |
| **«Багульник»**, «Барьер-3» | Чувствительный элемент — трибоэлектрический кабель КТМ-1,5 × 2, совмещенный с остроколючей спиралью АКЛ, размер зоны — 200 + 200 м, состав: спираль АКЛ, 4 кабеля КТМ, 2 устройства обработки, панель управления, стабилизатор напряжения, монтажный комплект | 24±12/9 В, 3 Вт |
| **«Крот»**, НПО «Техника» МВД РФ | Противоподкопное средство обнаружения на глубине 0,5–3 м, размер зоны — 25–200 м | 18–30 В |
| **«Цикорий»**, НПО «Техника» МВД РФ | Комплекс противоподкопных средств из 32 участков блокирования с глубиной обнаружения до 3 м, размер зоны — до 800 м | |

| 1 | 2 | 3 |
|---|---|---|
| **«Guardwire»**, Geoguip, Англия | Электромагнитный микрофонный кабель для легких металлических и деревянных оград, размер зоны — до 400 м, состав: микрофонный кабель, анализатор | 11–16 В, 100 мА |
| **S-103**, Safeguard Technology Inc., США | Сейсмодатчики для установки под асфальтом и бетоном через 3 м, размер зоны — 75 м, сейсмодатчики до 2 × 25 шт., процессор S-103 | 12 В |
| Волоконно-оптическая система сигнализации **«Ворон»**, ЗАО «Этис-М», ЗАО НПО «Прикладная радиофизика — ОС» | Максимальная длина периметра зоны — 30 км, макс. число охраняемых зон — 56, длина охраняемой зоны — до 550 м, тип охраняемого ограждения — любые подвижные, обучение для конкретных ограждений, невосприимчивость к электромагнитным помехам | |

*Примечание.* КЧЭ — кабельный чувствительный элемент.

## 6. Извещатели емкостные

*Таблица П.3.6*

| *Тип извещателя* | *Назначение* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| **ИО 305-3 «Пик»** | Для блокировки сейфов, металлических шкафов, решеток, оконных, витринных и дверных проемов | Максимальная емкость ЧЭ, диапазон регулировки чувствительности — 0–0,2 м | 180 × 125 × 50 мм, 1,0 кг |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **ИО 305-4 «Граднент»** | Для блокировки поверхностей складских ангаров | Размеры зоны обнаружения: сечение — 0,6 × 2,5 м, протяженность — 5–500 м | 200 × 150 × 50 мм, 1,0 кг (без ЧЭ) |
| **«Радиан-14»**, **«Радиан-15»**, **«Радиан-14 НХ»**, ГУП СНПО «Элерон» | Для охраны периметров объектов с использованием козырькового и полноростового заграждений | Длина зоны обнаружения, вероятность обнаружения — 0,95 | |
| **«Раднан-М»**, ПО «Север» | Для установки на полновысотных металлических оградах и козырьках | Длина зоны обнаружения — 10–25 м | |
| **«E-Field»**, Stelar, США | Для охраны периметров | Длина зоны — 2 × 150 м, радиус — до 1 м | |

*Примечание.* ЧЭ — чувствительный элемент.

## 7. Извещатели пожарные

*Таблица П.3.7*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|
| *1* | *2* | *3* |
| Тепловой извещатель **ИП 101-2** | Защищаемая площадь — 25 м², t° срабатывания — 60° С, инерционность — 60 с | 110 × 95 мм, 200 г |
| Тепловой извещатель **ИП 103-4/1 «Мак»** | Защищаемая площадь — 15 м², t° срабатывания — 60–70° С, инерционность — 90 с | 60 × 65 мм, 200 г |

| 1 | 2 | 3 |
|---|---|---|
| Дымовой извещатель **ИП 212-5 (ДИП-3)** | Защищаемая площадь — 150 м², чувствительность — 0,05–0,5 дБ/м, инерционность — 5 с | 120 × 70 мм, 380 г |
| Дымовой линейный извещатель **ИП 212-7 (ИДПЛ-1)** | Защищаемая площадь — 1000 м², чувствительность — 1, 5 дБ/м | 100 × 100 × 125 мм, 1 кг |
| Световой извещатель **ИП 329-2 «Аметист»** | Защищаемая площадь — 300 м², чувствительность — 0,5 дБ/м, инерционность — 5 с | 140 × 255 мм, 0,8 кг |

## 8. Извещатели комбинированные

*Таблица П.3.8*

| *Тип извещателя* | *Основные характеристики* | *Габариты, масса, состав* |
|---|---|---|
| *1* | *2* | *3* |
| **ИО 40709-1 «Сокол-1»** | Типы извещателей — инфракрасный пассивный и радиоволновый активный, макс. дальность действия — 12 м, контролируемая площадь — 90 м², контролируемый объем — 150 м³, диапазон скоростей движения злоумышленника — 0,3–3 м/с | 160 × 125 × 125 мм, 0,9 кг |
| **ИО 414-1 «Сокол-2»** | Типы извещателей — инфракрасный пассивный и радиоволновой активный, макс. дальность — 15 м, контр. площадь — 120 м², диапазон скоростей движения злоумышленника — 0,3–3 м/с | 195 × 70 × 50 мм, 350 г |

| *1* | *2* | *3* |
|---|---|---|
| **DT 4201T, DT4351T, DT4501T** | Максимальная дальность действия 6, 11, 15 м*; контролируемая площадь — 20, 65, 125* м², угол обзора в вертикальной плоскости — 65°, скорость перемещения злоумышленника — 0,3–2 м/с | 130 × 70 × 60 мм, 350 г |
| **«Протва-4»**, ГУП СНПО «Элерон» | Типы датчиков — радиолучевые, вибрационные и линии вытекающей волны, размер зоны — до 7,5 км при 60 контролируемых участках от 50 до 125 м каждый с шириной зоны обнаружения до 6 м | До 60 датчиков каждого типа и блоков обработки сигналов, пульт управления и индикации, источники питания |
| **«Гардина-95»**, НИКИРЭТ | Типы извещателей — электроконтактные, емкостные, вибрационные, радиолучевые и др., размеры зоны — до 20 км (40 участков по 0, 5 км), до 4 ворот с дистанционно управляемыми замками | До 40 шкафов и блоков линейных, блок обработки, блок питания и щит вводной |
| **«Миля-2000»**, Центр внедрения систем безопасности ГУП СНПО «Элерон» | Типы извещателей — контактные (Миля-2000К), вибрационные (Миля-2000В), телемеханическая система сбора, обработки, представления и документирования информации, размер зоны — 2 фланга по 10 км | |

*Примечание.* *) — первое значение для DT4201T, второе — для DT4351T, третье — DT4501T.

## 9. Средства радиоконтроля

*Таблица П.3.9*

| *Тип средства (производитель)* | *Назначение* | *Основные технические характеристики* | *Габариты, масса* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| Многофункциональные портативные комплексы **АРК-Д1Т**, **АРК-Д1ТИ** (ЗАО «Иркос») | Радиоконтроль источников радиоизлучений УКВ диапазона, измерение, запись сигналов, пеленгование их источников | Диапазон частот — 9 кГц–18 ГГц (макс. конфигурация), чувствительность — 1–2 мкВ, скорость перестройки — 150 МГц/с, виды демодулированных сигналов — АМ, ЧМ, ОБПв, ОБПн, рабочий диапазон пеленгования — 25–1012 МГц, инструментальная точность пеленгования — 2°–5° | Устройства в атташекейсе, комплект антенн, Notebook, кейс-атташе с аксесссуарами |
| **«Крона-6000 М»** (НПЦ «Нелк») | Автоматическое обнаружение и определение местоположения радиоизлучающих устройств в помещении | Диапазон частот — 0,1–6000 МГц, мин. мощность источника излучения — 50 мкВт, ошибка определения местоположения — 10 см, генерация прицельной помехи в диапазоне 65–1000 МГц | Устройства в атташекейсе, Notebook, антенны, акустические колонки |
| **«Навигатор»** (НПЦ «Нелк») | Автоматизированное измерение побочных радиоизлучений | Диапазон частот — 9 кГц–1000 МГц, полосы пропускания — 1, 3, 10, 30, 100, 300 кГц, 1, 3 МГц, точность измерения уровня — 2% | Анализатор спектра, Notebook, комплект антенн |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Прибор обнаружения средств негласного съема информации **«OSC-5000»** (OSCOR) (Resefrch Bestronics Inc., США) | Обнаружение и локализация каналов утечки информации | Диапазон частот — 10 кГц–3 ГГц, 850–1070 нм (ИФК), 10 кГц–5 МГц (контроль сети электропитания), чувствительность — 0,8 мкВ (в полосе 15 кГц), вид модуляции сигналов AM, FMW, FMN, SS, SB/CW, динамический диапазон — 90 дБ | 473 × 368 × 159 мм, 12,7 кг |
| Автоматизированный комплекс для проведения специальных исследований **«Сигурд»** (ООО «Маском») | Проведение специальных исследований технических средств | Диапазон частот — 9 кГц–2,7 ГГц, автоматическое измерение и расчет радиусов зон, оценка защищенности технических средств (объектов) | Широкополосный предусилитель, спектроанализатор, ПЭВМ, антенны измерительные |
| Многофункциональный комплекс радиоконтроля **КРК-5М** (ОАО «Ново») | Автоматическое обнаружение и определение местоположения технических средств негласного контроля | Диапазон частот 0,01–6000 МГц (с конвертором), чувствительность — 1–2 мкВ, скорость обзора — 80 МГц/с, скорость анализа — 200 МГц/с, время сканирования в диапазоне 0,01–2600 МГц — 0,5–1 мин | Аппаратная часть в стандартном кейсе, ПЭВМ Notebook |
| Поисковый комплекс **«Дельта-П-08»** (ЦКБИ ГП «Элерон») | Автоматическое обнаружение и определение местоположения источников радиоизлучения | Диапазон частот — 0,1–2036 МГц, чувствительность — 1 мкВ, виды модуляции — AM, WFM, NFM, SSB (в том числе с инверсией спектра и частотными перестановками), проверка проводных линий | Кейсовая упаковка |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| Комплекс **KS1000/8** (Фирма «Радиосервис») | Обнаружение, идентификации, определение местоположения и нейтрализации подслушивающих устройств, передающих сигналы по радио- и проводным каналам | Рабочий диапазон — 50–2600 МГц, дальность обнаружения радиомикрофонов — 10 м, минимальное время анализа 1 ГГц — 11 мин, точность оценки координат радиомикрофона — 5 см | Кейсовая упаковка |
| Детектор поля **D 006** (ООО «Смерш Техникс») | Обнаружение радиоизлучающих специальных технических средств | Диапазон частот — 50–1000 МГц, чувствительность — 0,5–3 мВ, радиус обнаружения источника излучения — 1 м при его мощности 5 мВт | Габариты — 128 × 63 × 20 мм, 0,21 кг (основного блока) |
| Устройство обнаружения радиомикрофонов «**Пионер-М**» (НПО «Специальная техника и связь» МВД России) | Обнаружение радио микрофонов и слуховой контроль сигналов различных передающих средств | Диапазон частот — 0,5–1900 МГц, виды модуляции — AM, WFM, NFM, SSB, кол. каналов памяти — 50, дальность обнаружения радиосигналов — 15 м | Носимое |
| Приемник ближней зоны «**Скорпион-2**» (Лаборатория № 11 ОАО «Холдинговая компания «Электрозавод»») | Быстрое обнаружение источников излучения в ближней зоне | Диапазон частот — 30–2000 МГц, чувствительность — 25–500 мкВ, скорость перестройки — 200 МГц/с | Носимый |

| *1* | *2* | *3* | *4* |
|---|---|---|---|
| Обнаружитель скрытых видеокамер **«Айрис VCF-2000»** (НПЦ «Нелк») | Обнаружение работающих скрытых видеокамер | Расстояние обнаружения — до 5 м, время обнаружения — 1,5–5 мин | Габариты — 200 × 150 × 55 мм, вес — 1,65 кг |
| Программно-аппаратный комплекс **ST 0110** (ООО «Смерш Техникс») | Скрытное обнаружение работающих диктофонов | Дальность обнаружения диктофонов — 0,3–1, 5 м | |

## 10. Анализаторы проводных коммуникаций

*Таблица П.3.11*

| *Тип средства (производитель)* | *Назначение* | *Основные технические характеристики* | *Габариты, масса* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| Анализатор телефонных линий **«Аврора»** (ЗАО НПЦ «Фирма «Нелк»») | Обнаружение закладных устройств, подключенных к телефонным линиям | Выявление неоднородности линии, вызванной несанкционированным подключением к ней, путем подачи в линию зондирующих сигналов и анализа отраженных | 200 × 25050 мм, масса — 1 кг |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Аппаратура обследования проводных коммуникаций «**Лиана**» (ООО «Фирма «Радэп»») | Обнаружение средств негласного контроля, использующих провода, и сигналов случайных акустоэлектрических преобразователей | Диапазон частот — 0,5–10000 кГц, чувствительность приемника в полосе 0,3–3,5 кГц — 30 мкВ, максимальная длина обследуемой коммуникации — до 200 м | Масса в упаковке — 20 кг |
| Телефонное проверочное устройство **ТПУ-7** (ОАО «Ново») | Обнаружение гальванически подключенных к телефонным линиям средств съема информации | Обнаруживает: последовательно подключенные средства с сопротивление не менее 50 Ом, параллельно подключенные средства с сопротивлением до 20 МОм, низкочастотные и высокочастотные сигналы | Носимое устройство, укладываемое вместе с комплектующими в чемодан |
| Комплекс для анализа проводных линий «**Меридиан**» (ООО «Маском») | Комплексное обследование проводных линий на наличие гальванических подключений | Диапазон измеряемых расстояний — 12,5, 25, 50, 200, 400, 800, 1600, 3200, 6400, 12800, 25600 м, зондирующий импульс амплитудой 5 В длительностью 7–10 нс, разрешение — 2 см | |
| Анализатор параметров проводных коммуникаций **LBD-50** (ИКМЦ-1 — Группа защиты — «ЮТТА») | Поиск несанкционированных гальванических подключений подслушивающих устройств | Диапазоны измерений: токов утечки — 0,1–200 мА, сопротивления изоляции — 0,1–20 Мом, длина анализируемой линии — 50–800 м | 500 × 400 × 140 мм, 4 кг |

## 11. Устройства защиты слаботочных линий

*Таблица П.3.12*

| *Тип устройства* | *Объект защиты* | *Вид, способ защиты* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|---|---|
| **Корунд** | ТА | Пассивная, защита от микрофонного эффекта | Затухание ОС — до 60 дБ, ПС — 2 дБ (1000 Гц) | 40 × 13 × 10 мм |
| **МП-1А МП-1Ц** | Аналоговый ТА, цифровой ТА | Пассивная, акт. защита от микрофонного. эффекта и ВЧ-навязывания | Затухание ОС — 54 дБ, ПС — 2 дБ, уровень шума — 32 мВ (0,02–300 кГц) | 50 × 70 × 35 мм |
| **Грань-300** | ТА | Пассивная, защита от микрофонного эффекта, ВЧ-навязывания, блокирует парал. ТА | | 90 × 55 × 25 мм |
| **МП-2** | Громкоговорители Трансляционные сети | «Розовый» шум | Амплитуда шумового сигнала — 1,8 мВ | |
| **МП-3** | Цепь электропитания | Пассивная защита | | |
| **МП-4** | Вторичные часы | Активная защита | | |
| **МП-5** | Громкоговорители систем оповещения | | Ослабление ОС — 90 дБ (0,02–10 кГц) | |

*Примечание.* ТА — телефонный аппарат.

## 12. Средства защиты речевого сигнала в телефонных линиях связи

*Таблица П.3.13*

| *Тип средства (производитель)* | *Метод защиты* | *Характеристика стойкости защиты* | *Масса-габаритные характеристики* | *Примечание* |
|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* |
| **Грот (SCR-M1/2)** (ООО «Центр безопасности информации «Маском») | Частотные и временные перестановки, открытое распределение ключей, дополнительный 7-значный ключ для идентификации пользователя | Количество ключевых комбинаций — $2 \cdot 10^{18}$ | | |
| **Грот-АП** (ООО «Центр безопасности информации «Маском»») | Защита от подключения к телефонной линии путем передачи от абонентского ТА «Грот-АП-С» кодовой посылки | Количество комбинаций кода — $7{,}38 \cdot 10^{19}$ | 78 × 51 × 27 мм — «Грот-АП-А» (АТС), 120 × 26 × 122 мм — «Грот-АП-С» | |
| **СКР-511 «Референт»** (ЗАО «Дикси») | Передача цифровым фазоманипулированным шумоподобным сигналом, динамические кодировочные таблицы | Временная стойкость | Телефонный терминал размером 150 × 100 × 33 мм | Временная задержка — не более 100 мс, скорость передачи — 4800 бит/с |
| **Акцент** (ЗАО «НПЦ Фирма «Нелк»») | Перегрузка и блокирование работы ЗУ помехой, защита от ВЧ навязывания, определение подключенных ЗУ и ТА | | 55 × 140 × 200 мм | |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Щит** (ООО «Центр речевых технологий») | Маскировка речеподобной помехой на приемной стороне | | | Защита включается последовательно принимающим абонентом |

## 13. Средства акустического и виброакустической зашумления

*Таблица П.3.14*

| *Тип устройства (производитель)* | *Диапазон частот, Гц* | *Вид помехи* | *Число каналов (излучателей)* | *Мощность излучения* | *Габариты, масса* |
|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* |
| **Барои** (ЗАО НПЦ Фирма «Нелк») | 60–16000 | «белый шум», речеподобная, смесь помех | 4 (30 — пьезоэлектр., 7 — электромаг.) | 18 Вт на канал | 377 × 335 × 108 мм, 8,5 кг |
| **Соната-АВ** (ЗАО «Анна») | 175–5600 | | 12 (модель 1А), 20 (модель 1М) | превышение помех над сигналом — 10 дБ | 153 × 135 × 65 мм (1А), 230 × 193 × 65мм (1М) |
| **Шелест-4К** (ЗАО РНТ) | 170–5700 | | 4(16) | | |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| **ЛГШ-301** (ЗАО «Лаборатория ППШ») | 180–11300 | | | 1 Вт, 50 м$^3$ | 66 × 66 × 20мм, 0,1 кг — основной блок, 70 × 47 × 86 мм, 0,12 кг — блок питания, |
| **ЛГШ-401** (ЗАО «Лаборатория ППШ») | | | 1 (8 — виброакуст. каналов, 1 — акустический) | 1 Вт на акустический канал | 200 × 125 × 50 мм, 1 кг |
| **ВВ 301** (ЗАО «РНТ») | 80–10000 | речеподобная помеха | 6/10 | 20 м$^2$ — площадь, 15 м$^3$ — объем | |
| **«Шорох-1, 2»** (ООО «Маском») | 175–5600 | | | 57 Вт (Ш-1), 19 Вт (Ш-2) | Ш-1: 340 × 300 × 140 мм, 12 кг; Ш-2: 280 × 270 × 120 мм, 6 кг |
| **WNG 023** (ООО «СмерШ Техникс») | 400–8000 | «белый» шум | | 84 дБ — звуковое давление | 111 × 79 × 22 мм, 0,2 кг — основной блок, 180 × 150 × 54 мм, 0,65 кг — упаковка |
| **Заслон-2М** (НРО «Специальная техника и связь») | 200–5000 | | (25 — вибропреобразоват., 6 — акустич.) | (0,25–2,5) м — толщина бетонной плиты | |
| **Скит-МВА** (Лаборатория № 11 ОАО Холдинговая компания «Электрозавод») | 200–15000 | | 3 (18 — вибропреобраз., 2 — акуст. изл.) | 1,5 м — радиус зашумления на бетоне | |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| SI-3030 (ЗАО «Защита информации») | 125–6300 | | 3 (72 электромагнитн. излучат., 100 — акустич. излучат.на канал) | 360 Вт | |

## 14. Средства подавления радиоэлектронных и звукозаписывающих устройств

*Таблица П.3.15*

| *Тип средства (производитель)* | *Назначение* | *Параметры подавления* | *Вид помехи* | *Габариты, масса* |
|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* |
| **Шторм** (НПЦ «Нелк») | Нейтрализация диктофонов, радиомикрофонов, электронных стетоскопов и др. | Зона подавления ≥ 60°, радиус подавления ≥ 6 м | Речеподобный шум | Размеры — 460 × 350 × 120, масса —12 кг |
| **Сапфир** (ООО «Центр безопасности информации «Маском») | Подавление сигналов диктофонов | Зона подавления 80–90, радиус подавления 2–6 м | Речеподобный шум | Размещается в кейсе, сумке, под столом |
| **Барсетка** (ООО «Центр безопасности информации «Маском») | Подавление сигналов диктофонов | Радиус подавления — 1–3 м | Речеподобный шум | Размещается в сумке-барсетке |
| **Мозаика** (ООО «Центр безопасности информации «Маском») | Подавление сотовых телефонов (стандартов GSM, CDVA, AMPS, DAMPS, NMT) | Радиус подавления: 3–15 м («Мозаика»), 3–50 м («Мозаика-М»), плавная регулировка мощности | Заградительная помеха | Для работы в офисе |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **RS Jammer GSM 900/1800** (ООО «Научно-производственная фирма «Радиосервис») | Блокировка работы мобильных телефонов стандарта GSM | | | Для работы в офисе |
| **RS Jammini** (ООО «Научно-производственная фирма «Радиосервис») | Блокирование работы мобильных телефонов | 10–15 (гарантированная), предельная — 50 | Последоват. импульсов $\tau = 300$ мкс, плотность потока энергии в импульсе $\geq 10$ мкВт/см$^2$ | Размеры — 20 × 16 × 6 мм, масса — 500 г |
| **Дурман** (ООО «Фирма «Радэл») | Подавление входных сигналов лентопротяжных и цифровых диктофонов | Радиус для большинства диктофонов — не менее 10 м, экранированных — 0,8–2 м | | Камуфлирование в носимых и стационарных предметах |
| **Равнина-3** (ООО «Фирма «Радэл») | Перехват и прицельное подавление по частоте и направлению, подавление мобильных каналов | Диапазон частот — 1–3000 МГц, точность определения направления — 2–3°, мощность помехи — 500–2000 Вт | | Стационарная аппаратура |
| **Раднола** (ООО «Фирма «Радэл») | Радиоэлектронное подавление сигналов управления и сотовой связи | Диапазон частот — 20–1000 МГц, выходная мощность — 60–80 Вт | | Носимая и возимая, масса — 18 кг + (7–12,6) кг (аккумул.) |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Скит-МП** (Лаборатория № 11 ОАО Холдинговая компания «Электрозавод») | Предотвращение утечки информации по каналам сотовой связи стандартов GSM 900/1800 (EGSM), AMPS/DAMPS, CDMA | Диапазон частот — 840, 960, 1680, 1920 МГц, радиус действия — до 12 м | Шум в импульсном режиме | Для работы в офисе |
| **ЛГШ-102 «РаМЗес-Авто»** (ЗАО «Лаборатория ППШ») | Подавление сигналов записи в диктофонах | Зона подавления — 70° | Помеховый сигнал на f ≈ 500 МГц | Для работы в автомобиле и офисе |
| **ЛГШ-103** «РаМЗес – Дубль» (ЗАО «Лаборатория ППШ») | Подавление сигналов записи в диктофонах | Зона подавления —70°, расстояние подавление — 1,5 м | | Для работы в офисе |

## 15. Нелинейные локаторы

*Таблица П.3.16*

| *Тип локатора* | *Вид и частота излучений, МГц* | *Гармоники* | *Мощность излучения, Вт* | *Чувствительность, дБ* | *Габариты, масса* |
|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* |
| **Родник-2К** | непр., 980–1020 | 2 | 1 | –130 | 2,9 кг |
| **Родник-23** | имп., 910 | 2 и 3 | 0,03–2,5 — средн. | –150 | 15 кг (компл.) |
| **Онега -23М** | имп., 910 | 2 и 3 | имп. — 100/10, средн. — 1 | –120 | 206 × 145 × 65 мм, 3,2 кг |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| **NR-900EM** | имп., 900 | 2 и 3 | имп. — 150 | –129 | 4,5 кг |
| **NR-μ** | имп., непр., 848 | 2 и 3 | | –150 | 2,8 кг |
| **Orion** | непр., 915 | 2 и 3 | 0,014–1,4 | –130 | |
| **SEL SP-61 «Катран»** | непр., 885–895 | 2 и 3 | 0,08–1,5 | –127 | 4 кг |
| **Мастер** | имп. или непр., 980–1020 | 2 | сред. — 0,8 | –130 | 3 кг |
| **Мастер плюс** | имп. или непр. 980–1020 | 2 и 3 | сред. — 2 | –145 | 3,5 кг |
| **Обь-1** | непр., 1000 | 2 | 0,25 | –145 | 200 × 140 × 90 мм, 2,3 кг |
| **Циклон-М** | имп., 680 | 2 | 50–300 | –117 | 170 × 120 × 40 мм, 2,5 кг |
| **Люкс-3М** | имп., 915 | 2 | 20 | –135 | |
| **Super Broom**, Англия | непр., 888,5 | 2 и 3 | 0,014–1,4 | –127 | 18 кг |

## 16. Металлодетекторы

*Таблица П.3.17*

| *Тип металлодетектора (производитель)* | *Максимальная дальность обнаружения* | *Режим поиска* | *Индикация* | *Габариты, масса* | *Электропитание* |
|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* |
| **Корнет 7250, Кондор 7252** (Ака) | монета — 45 см, ПМ — 80 см | металлы | звуковая многотональная, визуальная (ЖК дисплей) | штанга — 1200 мм, э/блок — 138 × 108 × 80, 2,1 кг | аккумуляторы — 12 В, 1200 мА/ч |

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| **Сармат 7240, 7240М** (Ака) | монета — 35 см, ПМ — 70 см | металлы, цветные металлы | звуковая многотональная | штанга — 1200 мм, э/блок — 360 × 150 × 250, 1,7 кг | батарейки — 8(10) шт. |
| **Мииискаи 7210** (Ака) | ввнт М3 × 7 — 8 см, монета — 17 см, ПМ — 35 см | черные, цветные металлы | звуковая, световая | 165 × 82 × 32 мм, 260 г | батарейка 9 В |
| **7202** (Ака) | 5 мм обломок иглы — 5 см, ПМ — 30 см | металлы | звуковая, световая | 380 × 140 × 34 мм, 280 г | батарейка 9 В |
| **Унискаи 7215** (Ака) | ПМ — 40 см | металлы, цветные металлы | звуковая, световая | 380 × 140 × 34 мм, 280 г | батарейка 9 В |

*Примечание.* ПМ — пистолет Макарова.

## 17. Рентгеновские установки

*Таблица П.3.18*

| *Тип установки, производитель* | *Основные характеристики* | *Габариты, масса* |
|---|---|---|
| *1* | *2* | *3* |
| | ***1. Флуороскопы*** | |
| **ФП-1, ФП-2**, ЗФО МНПО «Спектр» | Рабочее напряжение рентгеновской трубки — 30–75 кВ, размер экрана — 200 × 200 мм (ФП-1), 100 × 100 мм (ФП-2), разрешение — 2 пары линий/мм, проникающая способность — 6 мм (сталь) | 3 кг (ФП-1), 2 кг (ФП-2) |

| *1* | *2* | *3* |
|---|---|---|
| **«Шмель –90/К»**, Флэш Электроиикс | Напряжеиие реитгеиовской трубки — 90 В, рабочее поле коитроля — ∅ 255 мм, проиикающая способиость — 5 мм (сталь, 50 мм (алюмииий), 75 мм бетои, разрешеиие — 4 пары лиий/мм | 6,5 кг (реитгеиовский аппарат), 2,9 кг (просмотровое устройство) |
| ***2. Мобильные рентгенотелевизионные установки*** | | |
| **«Шмель-100ТВ»** | Напряжеиие на реитгеиовской трубке — 100 кВ, проникающая способиость — 10 см (сталь), 35 (алюмииий), рабочее поле — 180 × 240 мм, кол. запомииаемых изображеиий — 5000, разрешение — 768 × 570 пикселей | 6,2 кг — реитгеиовский аппарат, 3,1 кг — преобразователь, 8,5 — блок управлеиия и обработки изображеиий |
| **«Шмель-240 ТВ»** | Напряжеиие иа реитгеиовской трубке — 240 кВ, проникающая способиость — 19 мм (сталь), 72 (алюмииий), рабочее поле — 240 × 320 мм, кол. запоминаемых изображеиий — 5000, разрешеиие — 768 × 570 пикселей | 8,9 кг — реитгеиовский аппарат, 3,5 кг — преобразователь, 8,0 кг — блок управлеиия и обработки изображеиия |
| **«Очертание-ТВ»** («Шелест») | Напряжеиие на реитгеиовской трубке — 75/100 кВ, проиикающая способность — 10 мм (сталь), 40 мм (алюминий), рабочее поле — 250 × 250 мм, 320 × 420 мм | 12 кг — реитгеиовский аппарат, 4–6 кг — преобразователь, 9 кг — блок управлеиия и обработки изображеиий |
| **«Норка»** | Напряжение иа реитгеиовской трубке — 20–100 кВ, проиикающая способиость — 10/8 мм (сталь), 40/30 мм (алюминий), рабочее поле — 110 × 150, 290 × 390, 410 × 545 мм, разрешение — медная проволока толщиной 0,1 мм | Масса комплекса — 15 кг |
| **«Премьер»** | Напряжеиие иа реитгеновской трубке — 20–100/150 кВ, разрешающая способиость — медная проволока толщиной 0,1 мм, проникающая способность — 50/65 мм (алюминий), время экспозиции — 8 с | Масса комплекса — 35 кг |

## 18. Средства подавления радиоэлектронных и звукозаписывающих устройств

*Таблица П.3.19*

| *Тип средства (производитель)* | *Назначение* | *Параметры подавления* | *Вид помехи* | *Габариты, масса* |
|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* |
| **Шторм** (НПЦ «Нелк») | Нейтрализация диктофоиов, радиомикрофоиов, электроиых стетоскопов и др. | Зона подавления ≥ 60°, радиус подавления ≥ 6 м | Речеподобный шум | 460 × 350 × 120 мм, 12 кг |
| **Сапфир** (ООО «Цеитр безопасиости ииформации «Маском») | Подавлеиие сигиалов диктофоиов | Зоиа подавления 80–90, радиус подавления 2–6 м | Речеподобный шум | Размещается в кейсе, сумке, под столом |
| **Барсетка** (ООО «Цеитр безопасиости ииформации «Маском») | Подавление сигиалов диктофоиов | Радиус подавления — 1–3 м | Речеподобный шум | Размещается в сумке-барсетке |
| **Мозаика** (ООО «Цеитр безопасиости ииформации «Маском») | Подавлеиие сотовых телефоиов (стаидартов GSM, CDVA, AMPS, DAMPS, NMT) | Радиус подавления: 3–15 м («Мозаика»), 3–50 м («Мозаика-М»), плавная регулировка мощности | Заградительная помеха | Для работы в офисе |
| **RS Jammer GSM 900/1800** (ООО «Научио-производствеииая фирма «Радиосервис») | Блокировка работы мобильиых телефоиов стаидарта GSM | | | Для работы в офисе |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **RS Jammini** (ООО «Научно-производственная фирма «Радиосервис») | Блокирование работы мобильных телефонов | 10–15 м (гарантированная), предельная — 50 м | Последовательность импульсов длит.300 мкс, плотность потока энергии в импульсе — ≥10 мкВт/см$^2$ | Размеры — 20 × 16 × 6 мм, масса — 500 г |
| **Дурман** (ООО «Фирма «Радэл») | Подавление входных сигналов лентопротяжных и цифровых диктофонов | Радиус для большинства диктофонов — не менее 10 м, экранированных — 0,8–2 м | | Камуфлирование в носимых и стационарных предметах |
| **Равнина-3** (ООО «Фирма «Радэл») | Перехват и прицельное по частоте и направлению подавление мобильных каналов | Диапазон частот — 1–3000 МГц, точность опред. направления — 2–3°, мощность помехи — 500–2000 Вт | | Стационарная аппаратура |
| **Радиола** (ООО «Фирма «Радэл») | Радиоэлектронное подавление сигналов управления и сотовой связи | Диапазон частот — 20–1000 МГц, вых. Мощность — 60–80 Вт | | Носимая и возимая, масса — 18 кг + (7–12,6) кг (аккумул.) |
| **Скит-МП** (Лаборатория № 11 ОАО Холдинговая компания «Электрозавод») | Предотвращение утечки информации по каналам сотовой связи стандартов GSM 900/1800 (EGSM), AMPS/DAMPS, CDMA | Диапазон частот — 840, 960, 1680, 1920 МГц, радиус действия — до 12 м | Шум в импульсном режиме | Для работы в офисе |

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **ЛГШ-102** «РаМЗес-Авто» (ЗАО «Лаборатория ППШ») | Подавлеиие сигналов записи в диктофонах | Зона подавления — 70° | Помеховый сигиал на f ≈ 500 МГц | Для работы в автомобиле и офисе |
| **ЛГШ-103** «РаМЗес – Дубль» (ЗАО «Лаборатория ППШ») | Подавление сигналов записи в диктофонах | Зона подавления — 70°, расстояние подавление — 1,5 м | | Для работы в офисе |

## 19. Средства уничтожения информации на машинных носителях

*Таблица П.3.20*

| *Тип (производитель)* | *Назначение* | *Основные характеристики* |
|---|---|---|
| *1* | *2* | *3* |
| **«Стек-НС2» (Модель «М»)** (ЗАО «Аина») | Экстреииое уничтожеиие иформации на виичестерах | Напряжеииость стирающего магиитного поля ≥ 380 кА/м, габариты рабочей камеры — 185 × 108 × 30 мм, время стираиия — ие более 0,1 с, время между повториыми стираииями — 5 мин, кол. рабочих камер — 1 |
| **«Стек-КДС1»** (ЗАО «Аииа») | Быстрое стирание информации на большом количестве магиитных дисков | Напряжениость стирающего магиитного поля ≥ 330 кА/м, время стирания информации — не более 0,1 с, время готовиости после подачи питаиия — ие более 20 мии, габариты рабочей камеры — 100 × 99 × 13 мм, количество рабочих камер — 1 |

| 1 | 2 | 3 |
|---|---|---|
| **«Стек-НС1»** (ЗАО «Аииа») | Быстрое стираиие иифор-мации иа большом коли-честве магиитиых дисков | Напряжеииость стирающего магиитиого поля ≥ 400 кА/м, время стираиия ииформации — ие более 0,1 с, время го-товиости после подачи питаиия — не более 10 мии, габа-риты рабочей камеры — 200 × 120 × 39 мм, количество ка-мер — 1 |
| **«Страйкер»** (НПЦ «Нелк») | Быстрое стирание инфор-мации иа магиитиых ио-сителях, фуикциоиирую-щих в момеит стираиия | Напряжеииости стирающего магиитиого поля ≥ 350 кА/м, время готовиости после подачи питаиия — ие более 6 мии, время стираиия — ие более 0,1 с, количество и размеры ра-бочих камер зависят от типа иосителя |
| **СГУ-1** (Специализи-роваииый цеитр про-граммных систем «Спектр») | Уиичтожеиие ииформа-ции иа магнитиых иосите-лях и в памяти ЭВМ | Программный комплекс для ЭВМ типа IBM PC |

## 20. Специальные ЭВМ в защищенном исполнении

*Таблица П.3.21*

| *Тип ЭВМ (производитель)* | *Назначение* | *Основные технические характеристики* |
|---|---|---|
| 1 | 2 | 3 |
| Защищеииая ПЭВМ **«Об-руч»** (ЗАО «РНТ») | Обработка ииформа-ции с грифом «Сек-ретио» и «Совершеи-иио секретно» | Процессор — Intel Pentium III 800 МГц, память — до 768 Мб, слоты — 4 × PCI + AGP, иакопители — FDD, HDD — 20 Гб, CD-ROM, защита иа расстояиии 5 м, все ма-шииные носители — съемные для храиеиия их в сейфах |

| *1* | *2* | *3* |
|---|---|---|
| Защищенная ПЭВМ **«Flagman-Z»** (ЗАО «Ниеншанц-Защита») | Обработка информации на объектах 2-й категории | Радиус перехвата не менее 10 м, НЖД размещается в съемных блоках, устанавливаются программно-аппаратные средства защиты |
| Защищенные компьютеры марки **CLR** (ООО «УСП Компьюлинк») | Обработка и хранение секретной информации | Уровень ПЕМИН соответствует нормам для ЭВТ и АСУ, комплектуются аппаратными шифраторами «Криптон», двойным кодовым замком на включение, электронными замками, генераторами шумов и др. |
| Защищенные ЭВМ серии **«Багет-11-05/-11-06»** (Конструкторское бюро «Корунд-М») | Обработка конфиденциальной информации на рабочих местах операторов | Процессор — 486 DX4 133, ОЗУ — 32 Мбайт, жесткий диск — не менее 2 Гбайт, разрешение SVGA — 1280 × 1024, экранирование ПЭМИН, радиус перехвата радиосигналов — не более 10 м |
| Многопроцессорная ЭВМ **«Багет-01-09»** (Конструкторское бюро «Корунд-М») | Обработка конфиденциальной информации в сервере | Корпус металлический, обеспечивающий электромагнитное экранирование побочных излучений |
| Изделие защиты персональных компьютеров **«Салют»** (ЗАО Научно-техническая фирма «Криптон НИИАА») | Защита информации, обрабатываемой на ПЭВМ | Изучение вокруг компьютера электромагнитного помехового поля, формируемого из изменяющейся по случайному закону видеоинформации со строчными и кадровыми синхроимпульсами. Выпускается для шин ISA и PCI |

## 21. Средства защиты цепей питания и заземления

*Таблица П.3.22*

| *Тип средства (производитель)* | *Назначение* | *Технические характеристики* | *Эксплуатационные характеристики* |
|---|---|---|---|
| **Соната-С1** (ЗАО «Анна») | Линейное зашумление цепей электропитания | Количество «зашумляемых» сетевых каналов — 1, полоса частот шума — 0,01–30 МГц | |
| **Импульс** (НПЦ «Нелк») | Линейное зашумление цепей электропитания | Полоса частот шума — 0,02–10 МГц, максимальная мощность помехи — 9 Вт | Габариты — 195 × 145 × 62 мм |
| **Фаза-1-5, Фаза-1-10** (НПЦ «Нелк») | Подавление опасных сигналов в цепях электропитания | Ф-1-5: кол. потребителей — 2, эффект. подавления — 30–120 дБ, нагрузочная способность — 1500 ВА; Ф-1-10: кол. потребителей — 3, эффект. подавления — 40–150 дБ, нагрузочная способность — 2000 ВА | Масса — 2,4 кг (Фаза-1-5), 1,4 кг (Фаза-1-10) |
| **Скит-МС** (Лаборатория № 11 ОАО Холдинговая компания «Электрозавод») | Линейное зашумление цепей электропитания | Кол. каналов — 2, полоса частот помех — 30–300 кГц, мощность помехи — 1,0 Вт | |
| **ЛГШ-220** (ЗАО «Лаборатория ППШ») | Линейное зашумление цепей электропитания | Генерируется псевдослучайная последовательность | |
| **ЛФС-40-1Ф** (ЗАО «Лаборатория ППШ») | | Затухание в полосе диапазоне частот 0,1–1000 МГц — не менее 60 дБ, падение напряжения на f = 50 Гц и I = 40 А — не более 0,3 В | Габариты — 430 × 150 × 85 мм, масса — не более 4 кг |

## 22. Системы экранирования и комплексной защиты помещения

*Таблица П.3.23*

| *Тип системы (производитель)* | *Назначение* | *Основные технические характеристики* | *Габариты, масса* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| **Экранированные сооружения, помещения, камеры** (ООО «Малое внедренческое предприятие «Талисман») | Защита информации и обеспечения ЭМС в пунктах связи, вычислительных и аналитических центрах, помещениях, испытательных и исследовательских центрах и лабораториях, лабораториях для сертификации, медицинских диагностических центрах | Затухание электромагнитной энергии в диапазоне частот 10 кГц–100 ГГц — 60–120 дБ (стационарный и мобильный варианты) , 20 кГц–100 ГГц — 60–80 дБ (сборно-разборный вариант). Оборудованы защищенными: экранированными дверьми, воротами, проемами и средствами их сигнализациями; помехоподавляющими фильтрами, средствами вентиляции и кондиционирования; средствами пожарной сигнализации, пожаротушения и дымоулавливания | Варианты выполнения: стационарный — из стальных листов толщиной 2–3 мм, сборно-разборный — из стальных панелей размером 2300 × 1100 мм, мобильный — из стальных листов толщиной 2–3 мм на несущем каркасе размером 12 × 4 × 3,2 м |
| **Безэховые камеры (БЭК)** (ООО «Малое внедренческое предприятие «Талисман») | Проведение испытаний различных объектов на соответствие специальным требованиям по защите информации | Затухание электромагнитной энергии в диапазоне 20 кГц–100 ГГц — 60–120 дБ, уровень безэховости — до –40 дБ | |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Система комплексной защиты помещений «Скит-М» (Лаборатория № 11 ОАО Холдинговая компания «Электрозавод») | Предотвращение перехвата информации техническими средствами разведки | Виды зашумления: трехканальное виброакустическое, двухканальное линейное цепей электропитания, пространственное широкополосное электромагнитное, сигналов сотовой связи стандартов DAMPS, GSM 900/1800, CDMA | |

# Литература

## Основная литература


1. *Гарсиа М.* Проектирование и оценка систем физической защиты. Пер. с англ. — М.: АСТ, 2002.
2. *Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.* Энциклопедия промышленного шпионажа. — СПб.: Полигон, 2000.
3. *Меньшаков Ю. К.* Защита информации от технических средств разведки. — М.: РГГУ, 2002.
4. *Петраков А. В., Дорошенко П. С., Савлуков Н. В.* Охрана и защита современного предприятия. — М.: Энергоатомиздат, 1999.
5. Специальная техника и информационная безопасность: Учебник. Т. 1 / Под ред. *В. И. Кирина.* — М.: Академия управления МВД России, 2000.
6. *Торокин А. А.* Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
7. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998.
8. *Хорев А. А.* Теоретические основы оценки возможностей технических средств разведки. — М.: МО РФ, 2000.


## Дополнительная литература


1. *Абалмазов Э. И.* Направленные микрофоны. Мифы и реальность // Системы безопасности связи и телекоммуникаций. — 1996. — № 4.
2. *Абалмазов Э. И.* Новая технология защиты телефонных разговоров // Специальная техника. — 1998. — № 1.
3. *Абалмазов Э. П.* Пределы возможностей средств информационного поиска и защиты // Системы безопасности. — 1996. — № 1.
4. *Андрианов В. И., Соколов А. В.* «Шпионские штучки-2», или как сберечь свои секреты. — СПб.: Полигон, 1997.
5. Акустика: Справочник / Под ред. *М. А. Сапожкова.* — М.: Радио и связь, 1989.
6. *Арлащенков Ю. П., Ковалев М. С., Котов Н. Н., Тюрин Е. П.* Применение технических средств в борьбе с терроризмом. — М.: НИЦ «Охрана» ГУВО МВД России, 2000.
7. *Алексенцев А. И.* О классификации конфиденциальной информации по видам тайны // Безопасность информационных технологий. — 1999. — № 3. — С. 65–71.

8. *Алексенцев А. И.* Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. — 2000. — № 3. — С. 79–84.
9. *Алексеенко В. Н., Сокольский Б. В.* Система защиты коммерческих объектов. Технические средства защиты: Практическое пособие для предпринимателей и руководителей служб безопасности. — М., 1992.
10. *Алексеенко В. Н., Древс Ю. Г.* Основы построения систем защиты производственных предприятий и банков. — М.: МИФИ, 1996.
11. *Алексеенко В., Саржин А.* Организация проведения поисковых мероприятий. Специальная защита объектов: Пособие для сотрудников служб безопасности, руководителей деловых и коммерческих структур. — М.: Фирма «Росси Секьюрити», 1997.
12. *Арлащенков Ю. П., Ковалев М. С., Котов Н. Н., Тюрин Е. П.* Применение технических средств в борьбе с терроризмом. — М.: НИЦ «Охрана» ГУВО МВД России, 2000.
13. *Андреев С. П.* ИК-пассивные датчики охранной сигнализации. — 1998. — № 1. — С. 20–30.
14. *Андрианов В. И., Соколов А. В.* Устройства для защиты объектов информатизации: Справочное пособие. — М.: АСТ; СПб.: Полигон. — 2000.
15. *Афанасьев Н. В.* Комбинированные объемные извещатели для закрытых помещений // Системы безопасности связи и телекоммуникаций. —1999. — Январь-февраль. — С. 36–40.
16. *Ашимхин А. В., Рембовский А. М.* Выявление технических каналов утечки информации: методы, структура и характеристики средств // Специальная техника, специальный выпуск. — 2002.— С. 42–48.
17. *Балашов П. А.* Защита речевой информации на объекте // Конфидент. — 2000. — № 4–5. — С. 11–125.
18. *Барсуков В. С., Дворянкин С. В., Шеремет И. А.* Безопасность связи в каналах телекоммуникаций. Серия «Технология электронных коммуникаций». — М.: НИФ «Электронные знания», СП «Эко-Трендз», 1992. Т. 20.
19. *Барсуков В. С.* Безопасность: технологии, средства, услуги. —М.: КУДИЦ-ОБРАЗ, 2001.
20. *Барсуков В. С.* Чтобы сохранить информацию, ее необходимо уничтожить // Специальная техника. — № 6.— 2001. — С. 44–50.
21. *Барсуков В. С.* Интегральная защита информации // Специальная техника. — 2002. — № 5 (с. 42–49), № 6 (с. 47–53).

22. *Барсуков В. С.* Интегрированная защита специальных экранированных помещений // Специальная техника. — 2000. — № 1.
23. *Барсуков В. С.* Найти и обезвредить. Технические средства обнаружения угроз // Мир безопасности. — 1997. — № 8. — С. 38–42.
24. *Барсуков В. С.* Защита факсов // Частный сыск, охрана, безопасность. — 1995. — № 12. — С. 31–32.
25. Батарейки и аккумуляторы. Серия «Информационное издание». Вып. 1. — Киев: Наука и техника, 1995.
26. *Барсуков В. С., Водолазкий В. В.* Современные технологии безопасности. — М.: Нолидж, 2000.
27. *Барсуков В. С.* Биоключ — путь к безопасности // Специальная техника. — 2003. — № 2.
28. *Беляев Е. А., Лаврухин Ю. Н., Пицык В. В.* Государственная система защиты информации от технических разведок и от ее утечки по техническим каналам. Структура задачи и перспективы развития // Безопасность информационных технологий. — 2000. — № 3. — С. 25–39.
29. *Белоусов Е. Ф., Гордин Г. Т., Ульянов В. Ф.* Основы систем безопасности объектов: Учебное пособие. Ч. 1. Введение в системы охранной безопасности / Под ред. *Оленина Ю. А.* — Пенза: Изд-во Пензенского гос. ун-та. — 2000. — С. 96.
30. *Беседин Д. И., Боборыкин С. Н., Рыжиков С. С.* Предотвращение утечки информации, хранящейся в накопителях на жестких дисках // Специальная техника. — 2001. — № 1. — С. 41–46.
31. *Боборыкин С. Н., Рыжиков С. С.* Термохимическое уничтожение информации // Специальная техника. — 2002. — № 2. — С. 46–50.
32. *Брусницын Н. А.* Кто подслушивает президентов (От Сталина до Ельцина).— М.: Вита-Пресс, 2000.
33. *Василевский И. В.* От готовых комплексов к пользовательскому конструктору // Системы безопасности связи и телекоммуникаций. — 1996. — № 6. — С. 66–67.
34. *Васильев О.* Ускорение перестройки: комплекс RS1000 со сканером AR5000 // Бизнес и безопасность в России. — 1996. — № 4–5. — С. 12–13.
35. *Василевский И. В., Болдарев А. И.* Одолели «жучки»?.. Пора проводить «дезинсекцию» // Конфидент. — 2000. — № 4–5. — С. 90–95.
36. *Василевский И. В., Болдырев А. И.* Облава на «жучков»? Мы знаем, как это сделать // Конфидент. — 2000. — № 4–5. — С. 96–105.
37. *Варламов А. В., Кисиленко Г. А., Хореев А. А., Федоринов А. Н.* Технические средства видовой разведки / Под ред. *А. А. Хорева.* — М.: Москва, РВСН, 1997.

38. *Вартанесян В. А.* Радиоэлектронная разведка. — М.: Военное издательство, 1991.
39. *Вакин С. А., Шустов Л. Н.* Основы радиопротиводействия и радиотехнической разведки. — М.: Советское радио, 1968.
40. *Вахлаков В. Р.* Обеспечение защиты информации от непреднамеренного воздействия техническими средствами // Специальная техника. — 2002. — № 2. — С. 51–57.
41. *Вернигоров Н. С.* Нелинейный локатор — эффективное средство обеспечения безопасности в области утечки информации. Защита информации // Конфидент. — 1996. — № 1. — С. 67–70.
42. *Вернигоров Н. С.* Использование нелинейного локатора для раннего обнаружения устройств звукозаписи // Конфидент. — 2001. — № 4. — С. 50–54.
43. *Введенский Б. С.* Современные системы охраны периметров. Части 1–3 // Специальная техника. — 1999. — № 3–5.
44. *Вишняков С. М.* Сертификация технических средств и систем охраны. Технические условия // Системы безопасности связи и телекоммуникаций. — 2002. — Июнь-июль.— С. 42–45.
45. *Вовченко В. В.* Организация защиты речевой информации на объекте // Конфидент. — 1998. — № 6. — С. 49–57.
46. *Волгин М. Л.* Паразитные процессы в радиоэлектронной аппаратуре. — М.: Советское радио, 1981.
47. *Волобуев С. В.* Безопасность социологических систем. — Обнинск: Викинг, 2000.
48. *Волхонский В. В.* Устройства охранной сигнализации. — СПб.: Экополис и культура, 1999.
49. *Волхонский В. В.* Системы охранной сигнализации. — СПб.: Экополис и культура, 2000.
50. *Викторов А. Д., Генне В. И., Гончаров Э. В.* Побочные электромагнитные излучения персонального компьютера и защита информации. Защита информации // Конфидент. — 1995. — № 3. — С. 69–71.
51. *Вишняков С. М.* Защита дверных проемов. Анализ стандартов // Системы безопасности связи и телекоммуникаций. — 2001. — Август–сентябрь. — С. 22–25.
52. *Вишняков С. М.* Двери защитные. Разработка новых требований в нормативных документах // Система безопасности связи и телекоммуникаций. — 2000. — Июль–август. — С. 92–94.
53. *Вишняков С. М.* Системы комплексной безопасности: вопросы стандартизации // Конфидент. — 2002. — № 1. — С. 32–35.

54. *Веремчук В. С., Никитин А. А., Климов А. В.* Вибрационные извещатели для защиты строительных конструкций и сейфов // Системы безопасности связи и телекоммуникаций. — 1999. — Сентябрь–октябрь. — С. 32–37.
55. *Веремчук В. С., Никитин А. А., Климов А. В.* Акустические извещатели разрушения стекла. Нормативные аспекты развития // Системы безопасности связи и телекоммуникаций. — 1999. — Ноябрь–декабрь. — С. 44–49.
56. *Вернигоров Н.* Положите трубку. Вас подслушивают. Защита телефонных коммуникаций от несанкционированного съема информации // Частный сыск, охрана, безопасность. — 1996. — № 10. — С. 29–31.
57. *Волобуев С. В.* Безопасность социологических систем. — Обнинск: Викинг, 2000.
58. *Волокитин А. В., Маношкин А. П., Солдатенков А. В., Савченко С. А., Петров Ю. А.* Информационная безопасность государственных организаций и коммерческих фирм: Справочное пособие. — М.: НТЦ «ФИОРД-ИНФО», 2002.
59. *Волков В. Г.* Наголовные приборы ночного видения // Специальиая техника. — 2002. — № 5. — С. 2–15.
60. *Волхонский В. В.* Устройства охранной сигнализации. — СПб.: Экополис и культура, 1999.
61. Выбор и применение телевизионных систем видеоконтроля. Рекомендации. — М.: ВНИИПО МВД России, НИЦ «Охрана», 1996.
62. Выбор и применение современных средств охранно-пожарной синхронизации на объектах народного хозяйства. Рекомендации. — М.: ВНИИПО МВД СССР, 1991.
63. *Выходец А. В., Коваленко В. И., Кохно М. Т.* Звуковое и телевизионное вещание. — М.: Радио и связь, 1987.
64. *Гавриш В.* Практическое пособие по защите коммерческой тайны. — Симферополь: Таврида, 1994.
65. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. В 2-х кн. — М.: Энергоатомиздат, 1994.
66. *Гаценко О. Ю.* Защита информации Основы организационного управления. — СПб: Сентябрь, 2001.
67. *Гедзберг Ю.* Выбор объективов // БДИ. — 1997. — № 4. — С. 32–35.
68. *Гретченко О. И.* Проблема выбора. Защита иинформации // Конфидент. — 1997. — № 3. — С. 75–61.

69. *Громов Ю.* Формирование интегрированных систем безопасности // БДИ. — 1997. — № 2. — С. 27–29.
70. *Горохов П. К.* Толковый словарь по радиоэлектронике. Основные термины. — М.: Русский язык, 1993.
71. ГОСТ Р 50862-96. Сейфы и хранилища ценностей. Требования и методы испытаний и огнестойкость. — М.: Госстандарт России, 1996.
72. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. — М.: Госстандарт России, 1996.
73. *Давыдов Ю. Л.* Средства и системы для защиты периметров объектов // Системы безопасности связи и телекоммуникаций. — 1999. — № 2. — С. 32–36.
74. *Дайлов А. А., Кишкин В. А.* Хранилище ценностей // Системы безопасности. — 1996. — № 1. — С. 68–70.
75. *Дворянкин С. В., Клочкова Е. Н., Калужин Р. В.* Маскирование речевых сообщений на основе современных компьютерных технологий // Специальная техника. — 2001. — № 3.
76. *Девойно С.* Безопасность телефонных переговоров — проблема, имеющая решение // Частный сыск, охрана, безопасность. — 1995. — № 5.
77. *Девянин П. Н., Михальский О. О., Правиков Д. И., Щербаков А. Ю.* Теоретические основы компьютерной безопасности: Учебное пособие. — М.: Радио и связь, 2000.
78. *Демидов А. Е.* «Штивер»: уверенный взгляд из-за стекла // Системы безопасности связи и телекоммуникаций. — 1996. — № 3. — С. 24–25.
79. *Дориченко С. А., Ященко В. В.* 25 этюдов о шифрах. — М.: ТЕИС, 1994.
80. *Елисеев А. А.* Средства защиты слаботочных линий // Специальная техника. — 2000. — № 1.
81. *Ефимов А. И., Вихорев С. В.* Обеспечение информационной безопасности // Системы безопасности связи и телекоммуникаций. — 1996. — № 3. — С. 82–83.
82. *Жариков В. Ф., Киреев А. М., Синелев Д. В., Хмелев Л. С.* Тестовые режимы. Защита информации // Конфидент. — 1996. — № 2. — С. 49–52.
83. *Жаров А. А., Столбов М. Б.* Трудно искать диктофон в темном кармане... особенно если у вас нет PTRO 018. Защита информации // Конфидент. — 1997. — № 31. — С. 55–58.
84. *Железняк В. К., Макаров В. К., Хорев А. А.* Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. — 2000. — № 4.

85. *Жуков В. Ф.* Основы организации защиты информации. — М.: Издательство «ВиЛ», 2002.
86. *Журавленко Н. И., Курбанов Д. А.* Теория и методология защиты информации: Учебное пособие. — Уфа: Оперативная полиграфия, 2001.
87. *Завгородний В. И.* Комплексная защита информации в компьютерных системах: Учебное пособие. — М.: Логос, ПБОЮЛ Н. А. Егоров, 2001.
88. *Заличев Н. Н.* Энтропия информации и сущность жизни. — М.: Радиоэлектроника, 1995.
89. Закон РФ «О государственной тайне», № 5485-1 от 21.07.1993.
90. *Звежинский С.* Проблема выбора периметровых средств обнаружения // БДИ. — 2002. — № 8. — С. 36–41.
91. *Землянов В. М.* Своя контрразведка: Практическое пособие /Под ред. *А. Е. Тараса.* — Минск.: Харвест, 2004.
92. *Златопольский А. И.* Светопрозрачные защитные пленки: безопасность и комфорт // Системы связи связи и телекоммуникаций. — 1997. — № 2. — С. 74–75.
93. *Иванов И. В.* Периметр — первый рубеж охраны. Из опыта проектирования, монтажа и эксплуатации // Системы безопасности. — 1996. — № 1. — С. 46–53.
94. *Иванов И. В.* Охрана периметров — 2. — М.: Паритет Граф, 2000.
95. *Иванов Ю.* Фототехника для служб безопасности // Бизнес и безопасность в России. — 1997. — № 1. — С. 12–13.
96. Информационная безопасность. Том VIII. Оружие и технологии России. Энциклопедия. XXI век. — М.: Оружие и технологии, 2003.
97. *Исхаков Б. С., Каргашин В. Л., Юдин Л. М.* Подавление диктофонов: возможности и практическое применение // Специальная техника. — 2001. — № 5.
98. *Калинин С. В.* О некоторых новых тенденциях в развитии систем виброакустического зашумления // Конфидент. — 1999. — № 4–5. — С. 74–79.
99. *Калинин С. В.* Виброакустическое зашумление помещений — иллюзии и реальность // Конфидент. — 2001. — № 4. — С. 37–42.
100. *Калинцев Ю. К.* Криптозащита сообщений в системах связи: Учебное пособие. — М.: МТУСИ, 2000.
101. *Каргашин В. Л.* Проблемы обнаружения и идентификации средств негласного контроля информации. Часть 1–3 // Специальная техника. — 2000. — № 3–5.

102. *Каргашин В. Л.* Некоторые особенности реализации пассивных мер защиты в виброакустических каналах утечки речевой информации // Специальная техника. — 2002. — № 4. — С. 47–54.
103. Каталог продукции ЗАО «Анна», 2003.
104. Каталог продукции Евро-Азиатской ассоциации производителей товаров и услуг в области безопасности (ЕВРАС). Средства и системы безопасности, 2003.
105. Каталог техники. — М.: Фирма «РЭЙ-Защита информации», 2003.
106. Каталог фирмы SET-1, 2003.
107. *Кириллов Д.* Ценная информация всегда в цене // Частный сыск, охрана, безопасность. — 1996. — № 7. — С. 26–30.
108. *Кислов Р. И.* Экономические аспекты управления информационными рисками // Конфидент. — № 4–5. — 2002. — С. 116–121.
109. *Ковалев А. В.* Поисковые технические средства на основе методов интроскопии. Рентгеновские системы // Специальная техника. — 1999. — № 5. — Ч. 1, № 6. — Ч. 2; 2000. — № 1. — Ч. 3.
110. *Ковалев М. С. Шакиров Ф. А.* Системы охранного телевидения (Телевизионные системы видеонаблюдения). — М.: НПО «Защита информации», 2002.
111. *Климов А. В., Никитин А. А., Афанасьев Н. В.* Контактные извещатели разрушения стекла // Системы безопасности связи и телекоммуникаций. — 1999. — № 1. — С. 18–22.
112. *Кравченко В. Б.* Защита речевой информации в каналах связи // Специальная техника. — 1999. — № 4–5.
113. *Кравченко В. Б., Чертопруд С. В.* Ремонт и безопасность // Мир безопасности. — 2001. — № 2. — С. 48–52.
114. *Краснюк Д. В., Хованский В. А.* Инженерно-техническая безопасность: Учебно-практическое пособие. — М.: Изд-во МЭСИ, 1999.
115. *Крахмалев А. К.* Средства и системы контроля и управления доступом: Учебное пособие. — М.: НИЦ «Охрана» ГУВО МВД России, 2003.
116. *Кузнецов Ю. В., Баев А. Б.* Методы измерения ПЭМИН: сравнительный анализ // Конфидент. — № 3. — С. 54–57.
117. *Кучко А.* С. Аэрофотография и специальные фотографические исследования. — М.: Недра, 1988.
118. *Колтовой Н. А.* Инструментарий систем замкнутого телевидения // Системы безопасности. — 1995. — № 3. — С. 12–16.
119. Комплексные системы безопасности. Каталог. — М.: Научно-производственный центр «Нелк», 2001.
120. *Кондратьев А. В.* Некоторые вопросы специальных исследований ПЭМИН // Конфидент. — 2002. — № 4–5. — С. 80–83.

121. *Котенев А. А., Лекарев С. В.* Современный энциклопедический словарь по безопасности. Секьюрити. — М.: Ягуар, 2001.
122. *Кириллов Д.* Ценная информация всегда в цене // Частный сыск, охрана, безопасность. — 1996. — № 7. — С. 26–30.
123. *Лагутин В. С., Петраков А. В.* Утечка и защита информации в телефонных каналах. — М.: Энергоатомиздат, 1996.
124. *Лаврова Н. П., Спеценко А. Ф.* Аэрофотосъемка. Аэрофотосъемочное оборудование. — М.: Недра, 1981.
125. *Ларин А. И., Звежинский С. С.* Заграждение как элемент комплекса технических средств охраны // Специальная техника. — 2002. — № 3.
126. *Линдсей П., Норман Д.* Переработка информации у человека. — М.: Мир, 1974.
127. *Логинов Н. А.* Актуальные вопросы радиоконтроля в Российской Федерации. — М.: Радио и связь, 2000.
128. *Лысов А. В., Остапенко А. Н.* Телефон и безопасность (Проблемы защиты информации в телефонных сетях). — СПб.: Лаборатория противодействия промышленному шпионажу, 1995.
129. *Лысов А. В.* Лазерные микрофоны — универсальное средство разведки или очередное поветрие моды. Защита информации // Конфидент. — 1997. — № 1. — С. 61–62.
130. *Николаенко Ю. С.* Противодействие радиотехнической разведке // Системы безопасности связи и телекоммуникаций. — 1995. — № 6. — С. 12–15.
131. *Макаров Г.* Современные охранно-пожарные системы сигнализации // Мир безопасности. — 1997. — № 7. — С. 50–51.
132. *Максимов Ю. Н., Сонников В. Г., Петров В. Г., Паршуткин А. В., Еремеев М. А.* Технические методы и средства защиты информации. — СПб.: Полигон, 2000.
133. *Малюк А. А, Пазизин С. В., Погожин Н. С.* Введение в защиту информации в автоматизированиых системах. — М.: Горячая линия-Телеком, 2001.
134. Методологические основы обеспечения информационной безопасности объекта // Конфидент. — 2000. — № 1. — С. 75–86.
135. *Мельников В. В.* Основы теории защиты информации в автоматизированных системах // Вопросы защиты информации. — 2000. — № 3. — С. 39–48.
136. *Мироничев С.* Коммерческая разведка и контрразведка, или промышленный шпионаж в России и методы борьбы с ними. — М.: Дружок, 1995.

137. *Михалев Л. А., Сергеев А. А., Новичков И. С., Сталенков С. Е.* Исследования побочных электромагнитных излучений технических средств // Системы безопасности связи и телекоммуникаций. — 2001. — Июнь–июль. — С. 50–53.
138. *Мальцев Н. В.* Системы контроля доступом // Системы безопасности. — 1996. — № 1. — С. 43–45.
139. *Макиенко А.* Разведать без разведки помогут информационно-аналитические методы в деятельности СБ // Частный сыск, охрана, безопасность. — 1995. — № 6. — С. 10–12.
140. *Мельников В. В.* Защита информации в компьютерных системах. — М: Финансы и статистика, 1997.
141. *Минаев В. А., Скрыль С. В., Фисун А. П., Потанин В. Е., Дворянкин С. В.* Основы информационной безопасности: Учебник. — Воронеж: Воронежский институт МВД России, 2000.
142. *Назаров С. А.* На всякий пожарный случай. Руководителю все о пожарах. — М.: Мир безопасности, 1999.
143. *Николаенко Ю. С.* Противодействие радиотехнической разведке // Системы безопасности связи и телекоммуникаций. — 1995. — № 6. — С. 12–15.
144. *Николаев А. Г., Перцов С. В.* Радиотеплолокация (пассивная радиолокация). — М.: Советское радио, 1984.
145. *Николаенко Ю. С.* Антенные устройства // Системы безопасности связи и телекоммуникаций. — 1996. — № 2. — С. 28–32.
146. *Никулин О. Ю., Петрушин А. Н.* Системы телевизионного наблюдения. — М.: Оберг-РБ, 1997.
147. Обзор активных технических средств защиты. Защита информации // Конфидент. — 1997. — № 6. — С. 61–63.
148. *Ожегов С. И.* Словарь русского языка. — М.: Советская энциклопедия, 1968.
149. *Орлов В. А., Петров В. И.* Приборы наблюдения ночью и при ограниченной видимости. — М.: Военное издательство, 1989.
150. *Олейников В. В.* Делайте бизнес надежным и безопасным. — Рыбинск: Рыбинский дом печати, 1997.
151. *Оптнер С. Л.* Системный анализ для решения деловых и промышленных проблем. — М.: Советское радио, 1969.
152. Охранные системы. Серия «Информационное издание». Вып. 4. — Киев: Наука и техника, 1996.
153. *Омельянчук А.* Пущать или не пущать? Этот вопрос решают системы контроля доступа // Мир безопасности. — 1997. — № 5. — С. 39–44.

154. *Отт Г.* Методы подавления шумов и помех в электронных системах. — М.: Мир, 1979.
155. *Палий А. И.* Радиоэлектронная борьба. — М.: Военное издательство, 1989.
156. *Партыка Т. Л., Попов И. И.* Информационная безопасность: Учебное пособие для студентов учреждений среднего профессионального образования. — М.: Форум; ИНФРА-М, 2002.
157. Перечень сведений, отнесенных к государственной тайне. Указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне», № 1203 от 30 ноября 1995.
158. *Петраков А. В.* Защита и охрана личности, собственности, информации: Справочное пособие. — М.: Радио и связь, 1997.
159. *Петраков А. В., Лагутин В. С.* Защита абонентского телетрафика. — М.: Радио и связь, 2001.
160. *Петраков А. В., Лагутин В. С.* Телеохрана. — М.: Энергоатомиздат, 1998.
161. *Петраков А. В., Лагутин В. С.* Защита абонентского телетрафика. — М.: Радио и связь, 2001.
162. *Пешков А. Ф., Виноградов А. Ф.* Современные фотоаппараты. — СПб.: BHV-Санкт-Петербург, 1998.
163. *Плэтт В.* Стратегическая разведка. Основные принципы. — М.: Форум, 1997.
164. *Поздняков Е. Н.* Защита объектов (Рекомендации для руководителей и сотрудников служб безопасности). — М.: Банковский деловой центр, 1997.
165. *Поляков В. Т.* Посвящение в радиоэлектронику. — М.: Радио и связь, 1988.
166. *Притыко С. М.* Нелинейная радиолокация: принцип действия, область применения, приборы и системы // Системы безопасности связи и телекоммуникаций. — 1995. — № 6. — С. 52–55.
167. *Попугаев Ю.* Телефонные переговоры: способы защиты // Частный сыск, охрана, безопасность. — 1995. — № 3. — С. 74–84.
168. *Пятачков А. Г.* Контроль состояния защиты объектов информатизации: рекомендации по проведению // Конфидент. — 2001. — № 5. — С. 80–85.
169. *Расторгуев С. П.* Абсолютная система защиты // Системы безопасности. — 1996. — Июнь–июль. — С. 56–58.
170. *Русанов Ю. А.* Кабельные системы сигнализации // Системы безопасности. — 1995. — № 4. — С. 31–32.

171. Радиолокационные станции воздушной разведки / Под ред. *Кондратенкова Г. С.* — М.: Воениздат, 1983.
172. *Рембовский А. М.* Автоматизированный радиоконтроль излучений: задачи и средства // Специальная техника, специальный выпуск. — 2002. — С. 2–6.
173. *Рембовский А. М.* Повышение эффективности поисковых средств автоматизированного радиомониторинга // Специальная техника. — 2003. — № 4. — С. 40–47.
174. *Ронин Р.* Своя разведка: способы вербовки агентуры, методы проникновения в психику, форсированное воздействие на личность, технические средства скрытого наблюдения и съема информации: Практическое пособие. — Минск: Харвест, 1998.
175. *Сафонов Ю. П., Белобородов А. А., Савченко И. В., Орлов В. П.* Прозрачные переговорные кабины. История, настоящее, перспективы. Защита информации // Конфидент. — 1997. — № 3. — С. 57–61.
176. *Свечков Л. М., Чурляев Ю. А.* Защита коммерческой тайны в производственно-предпринимательской деятельности. Кн. 1. — М.: Центральный институт повышения квалификации кадров авиационной промышленности, 1992.
177. *Семенов Д. В.* Нелинейная радиолокация: концепция NR // Специальная техника. — 1999. — № 1–2. — С. 17–22.
178. *Семенов В. Г., Новичков И. С., Сенькин В. М.* Новые возможности электромагнитного экранирования // Безопасность информационных технологий. — 2001. — № 1. — С. 46–52.
179. *Семкин С. Н., Семкин А. Н.* Основы информационной безопасности объектов обработки информации: Научно-практическое пособие. — Орел, 2000.
180. *Синилов В. Г.* Системы охранной, пожарной и охранно-пожарной сигнализации: Учебник для нач. проф. образования. — М.: ИРПО, ПрофОбрИздат, 2001.
181. Системы безопасности. Межотраслевой тематический каталог. — М.: Гротек, 2003.
182. *Скребнев В. И.* Подповерхностная локация: новые возможности // Специальная техника. — 1998. — № 1. — С. 9–10.
183. *Смирнов Н. В., Николаев В. М.* Установка пожаротушения: проблемы выбора // Системы безопасности связи ителекоммуникаций. — 1999. — Январь–февраль. — С. 84–90.
184. Современные технологии безопасности. Каталог. — М.: Центр безопасности информации «Маском», 2003.
185. *Соколов А. В., Степанюк О. М.* Методы информационной защиты объектов и компьютерных сетей. — М.: АСТ; СПб: Полигон, 2000.

186. *Соколов А. В., Степанюк О. М.* Защита от компьютерного терроризма: Справочное пособие. — СПб.: БХВ-Петербург, Арлит, 2002.
187. *Соловьева Н. М.* Фотокиноаппаратура и ее эксплуатация. — М.: Легпромбытиздат, 1992.
188. *Соломенко А. В., Зарубин В. С., Хатуаев В. У.* Структура систем и комплексов охранно-пожарной сигнализации в терминах и определениях // Системы безопасности связи и телекоммуникаций. — 1999. — Июль–август (с. 36–39), сентябрь–октябрь (с. 26–29).
189. *Соколов А. В., Степанюк О. М.* Методы информационной защиты объектов и компьютерных сетей. — М.: АСТ; СПб.: Полигон, 2000.
190. *Симонов С. В.* Методология анализа рисков в информационных системах // Конфидент. — 2001. — № 1. — С. 72–76.
191. *Симонов С. В.* Технологии и инструментарий для управления рисками // Информационный бюллетень Jet Info. — 2003. — № 2. — С. 32.
192. *Ситников С. С.* Алгоритм оснащения современного объекта охраны СКУД // Системы связи и телекоммуникаций. — 2002. — Июнь–июль. — С. 50–53.
193. *Соломоненко А. В.* Монтаж объектовых комплексов технических средств охранной, охранно-пожарной сигнализации: Учебное пособие. Монтаж электропроводок объектовых технических средств сигнализации. Ч. 1. — Воронеж: Воронежская высшая школа МВД России, 1997.
194. *Степанов Е. А., Корнеев И. К.* Информационная безопасность и защита информации: Учебное пособие. — М.: ИНФРА-М, 2001.
195. *Спирин А. А.* Волоконно-оптические сети: введение в технологию // Мир ПК. — 1994. — № 8.
196. Средства защиты в машиностроении. Расчет и проектирование: Справочник. — М.: Машиностроение, 1989.
197. Съем информации по виброакустическому каналу (подготовлена экспертной группой компании «Гротек») // Системы безопасности связи и телекоммуникаций. — 1995. — № 5. — С. 12–15.
198. Технические средства, применяемые в охранной деятельности. Учебное пособие. — М.: Школа охраны «Баярд», 1995.
199. *Степанков С. Е.* «Навигатор» ведет безопасным курсом // Системы безопасности связи и телекоммуникаций. — 1997. — № 4. — С. 82–83.
200. Справочная книга по светотехнике. — М.: Энергоатомиздат, 1995.
201. Справочная книга радиолюбителя-конструктора. Кн. 1. — М.: Радио и связь, 1993.

202. Справочник инженерно-технических работников и электромонтеров технических средств охранно-пожарной сигнализации. — М.: НИЦ «Охрана» ВНИИПО МВД России, 1997.
203. *Тарасов Ю. А.* Контрольно-пропускной режим на предприятии // Конфидент. — 2002. — № 1. — С. 55–61.
204. *Татарченко Н. В., Тимошенко С. В.* Биометрическая идентификация в интегрированных системх безопасности // Специальная техника. — 2002. — № 2.
205. *Тимец Б. В.* Сделайте свой офис безопасней. Защита информации // Конфидент. — 1997. — № 1. — С. 37–39.
206. Терминологические основы проблематики информационной безопасности. — М.: МГУ, 2001.
207. Технические средства радиомониторинга. Каталог — 2004. — М.: Компания «Иркос», 2003.
208. *Торокин А. А.* Основы информационно-технической защиты информации. — М.: Ось-89, 1998.
209. *Торокин А. А.* К вопросу о понятийном аппарате защиты информации // Безопасность информационных технологий. — 1998. — № 4.
210. *Торокин А. А.* Концепция инженерно-технической защиты информации. Тезисы докладов XXXIII Научно-методической конференции профессорско-преподавательского состава МТУСИ. — М.: Изд-во МТУСИ, 1999.
211. *Торокин А. А.* Теоретические аспекты защиты информации. Тезисы докладов конференции «Методы и технические средства обеспечения безопасности информации». — СПб: Изд-во СПбГТУ, 2000.
212. *Торокин А. А.* Свойства информации как предмета защиты. Материалы межрегиональной научно-практической конференции «Информация и безопасность». Вып. 2. — Воронеж: Воронежский Государственный технический университет. — 2002. — С. 123–128.
213. *Устинов Г. Н.* Основы информационной безопасности систем и передачи данных: Учебное пособие. — М.: СИНТЕГ, 2000.
214. *Ушаков А., Чанцов С. Д., Якуб Ю. А.* Проводная связь. — М.: Связь, 1970.
215. Философский словарь / Под ред. *И. Т. Фролова.* — М.: Издательство политической литературы, 1991.
216. *Филлипс П. Д., Мартин Э., Уилсон С. Л., Пржибоки М.* Введение в оценку биометрических систем // Открытые системы. — 2000. — № 3. — С. 21–27.
217. Федеральный закон «Об информации, информатизации и защите информации». Принят Государственной Думой 25 января 1995 г.

218. *Харкевич А. А.* Спектры и анализ. — М.: Государственное издательство физико-математической литературы, 1962.
219. *Харкевич А. А.* Теоретические основы радиосвязи. — М.: Государственное издательство технико-теоретической литературы, 1957.
220. *Халяпин Д. Б.* Вас подслушивают? Защищайтесь! — М.: Мир безопасности, 2001.
221. *Хорев А. А.* Технические средства и способы промышленного шпионажа. — М.: Дальснаб, 1997.
222. *Хорев А. А.* Способы и средства подавления несанкционированного перехвата информации с телефонных линий // Системы безопасности. — 2003. — Август–сентябрь. — С. 90–93.
223. *Хорев А. А.* Методы и средства поиска электронных устройств перехвата информации. — М.: МО РФ, 1998.
224. *Хорев А. А., Макаров Ю. К.* Методы защиты речевой информации и оценки их эффективности // Конфидент. — 2001. — № 4. — С. 22–33.
225. *Хорев А. А., Макаров Ю. К.* Оценка эффективности систем виброакустической маскировки // Вопросы защиты информации. — 2001. — № 1. — С. 21–28.
226. *Цветнов В. В., Демин В. П., Куприянов А. И.* Радиоэлектронная борьба: радиоразведка и радиопротиводействие. — М.: Изд-во МАИ, 1998.
227. *Черняк В. З.* Тайны промышленного шпионажа. — М.: Вече, 2002.
228. *Членов А. Н.* Ультразвуковые охранные и охранно-пожарные извещатели для закрытых помещений // Системы безопасности связи и телекоммуникаций. — 1999. — № 2. — С. 27–19.
229. *Шваб А. Й.* Электромагнитная совместимость. — М.: Энергоатомиздат, 1995.
230. *Шеннон К.* Математическая теория связи. Работы по теории информации и кибернетике. — М.: Издательство иностранной литературы, 1963.
231. *Шелест С. О.* Методы и приборы для измерения параметров линии. Защита информации // Конфидент. — 1996. — № 4. — С. 57–60, 67–68.
232. *Шелест С. О.* Определение незаконных подключений к сети. Защита информации // Конфидент. — 1996. — № 5. — С. 63–65.
233. *Шрейдер Ю. А.* О семантических аспектах теории информации. В кн.: Информация и кибернетика. — М.: Советское радио, 1967.
234. *Шпак В. Ф.* Коммерческая тайна и экономическая безопасность бизнеса // Конфидент. — 2003. — № 2. — С. 20–26.

235. «Шпионские штучки» и устройства для защиты объектов и иифор-мации: Справочное пособие. — СПб.: Лань, 1996.
236. *Шарле Д. Л.* По всему земному шару. Прошлое, настоящее и будущее кабелей связи. — М.: Радио и связь, 1985.
237. *Юрьев С.* Сейфы и хранилища ценностей. Опыт сертитфикации на устойчивость к взлому // БДИ. — 1997. — № 2. — С. 99–101.
238. Электромагнитная совместимость радиоэлектрониых средств и непреднамеренные помехи / Сост. *Д. Р. Ж. Уайт.* Вып. 1–3. — М.: Советское радио, 1977, вып. 1; 1978, вып. 2; 1979, вып. 3.
239. *Ярочкин В. И.* Служба безопасности коммерческого предприятия. Организационные вопросы. — М.: Ось-89, 1995.
240. *Яглом А. М., Яглом И. М.* Вероятность и информация. — М.: Наука, 1973.
241. *Ярочкин В. И.* Безопасность информационных систем. — М.: Ось-89, 1996.
242. *Ярочкин В. И.* Коммерческая информация фирмы. Утечка, или разглашение конфиденциальной информации. — М.: Ось-89, 1997.
243. *Ярочкин В. И., Шевцова Т. А.* Словарь терминов и определений по безопасности информации. — М.: Ось-89, 1996.
244. *Ярочкин В. И.* Система безопасности фирмы. — М.: Ось-89, 1997.

# Оглавление

**ВВЕДЕНИЕ** ..... **3**

**РАЗДЕЛ I. КОНЦЕПЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ** ..... **8**

**Глава 1. Системный подход к инженерно-технической защите информации** ..... **10**

1.1. Основные положения системного подхода к инженерно-технической защите информации ..... 10

1.2. Цели, задачи и ресурсы системы защиты информации ..... 19

1.3. Угрозы безопасности информации и меры по их предотвращению ..... 23

**Глава 2. Основные положения концепции инженерно-технической защиты информации** ..... **29**

2.1. Принципы инженерно-технической защиты информации ..... 29

2.2. Принципы построения системы инженерно-технической защиты информации ..... 31

**Основные положения раздела I** ..... **42**

**РАЗДЕЛ II. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ** ..... **47**

**Глава 3. Характеристика защищаемой информации** ..... **47**

3.1. Понятие о защищаемой информации ..... 47

3.2. Виды защищаемой информации ..... 53

3.3. Демаскирующие признаки объектов защиты ..... 55

3.3.1. Классификация демаскирующих признаков объектов защиты ..... 56

3.3.2. Видовые демаскирующие признаки ..... 60

3.3.3. Демаскирующие признаки сигналов ..... 67

3.3.4. Демаскирующие признаки веществ ..... 73

3.4. Свойства информации как предмета защиты ..... 77
3.5. Носители и источники информации ..... 92
3.6. Запись и съем информации с ее носителя ..... 98

**Глава 4. Характеристика угроз безопасности информации... 104**

4.1. Виды угроз безопасности информации ..... 104
4.2. Источники угроз безопасности информации ..... 112
4.3. Опасные сигналы и их источники ..... 122

**Глава 5. Побочные электромагнитные излучения и наводки ..... 129**

5.1. Побочные преобразования акустических сигналов в электрические сигналы ..... 130
5.2. Паразитные связи и наводки ..... 137
5.3. Низкочастотные и высокочастотные излучения технических средств ..... 145
5.4. Электромагнитные излучения сосредоточенных источников ..... 155
5.5. Электромагнитные излучения распределенных источников ..... 158
5.6. Утечка информации по цепям электропитания ..... 161
5.7. Утечка информации по цепям заземления ..... 166

**Глава 6. Технические каналы утечки информации ..... 169**

6.1. Особенности утечки информации ..... 169
6.2. Типовая структура и виды технических каналов утечки информации ..... 171
6.3. Основные показатели технических каналов утечки информации ..... 180
6.4. Комплексное использование технических каналов утечки информации ..... 190
6.5. Акустические каналы утечки информации ..... 194
6.6. Оптические каналы утечки информации ..... 210

6.7. Радиоэлектронные каналы утечки информации ..... 222
6.7.1. Виды радиоэлектронных каналов утечки информации ..... 222
6.7.2. Распространение опасных электрических и радиосигналов в радиоэлектронном канале утечки информации ..... 226
6.8. Вещественные каналы утечки информации ..... 242
6.8.1. Общая характеристика вещественного канала утечки информации ..... 242
6.8.2. Методы добывания информации о вещественных признаках ..... 246
**Глава 7. Методы добывания информации ..... 253**
7.1. Основные принципы разведки ..... 253
7.2. Классификация технической разведки ..... 256
7.3. Технология добывания информации ..... 260
7.4. Способы доступа органов добывания к источникам информации ..... 266
7.5. Показатели эффективности добывания информации ..... 273
**Глава 8. Методы инженерно-технической защиты информации ..... 280**
8.1. Факторы обеспечения защиты информации от угроз воздействия ..... 280
8.2. Факторы обеспечения защиты информации от угроз утечки информации ..... 282
8.3. Классификация методов инженерно-технической защиты информации ..... 287
**Глава 9. Методы физической защиты информации ..... 300**
9.1. Категорирование объектов защиты ..... 300
9.2. Характеристика методов физической защиты информации ..... 302

**Глава 10. Методы противодействия наблюдению ..... 312**
10.1. Методы противодействия наблюдению в оптическом диапазоне ..... 312
10.2. Методы противодействия радиолокационному и гидроакустическому наблюдению ..... 320
**Глава 11. Методы противодействия подслушиванию ..... 323**
11.1. Структурное скрытие речевой информации в каналах связи ..... 323
11.2. Энергетическое скрытие акустического сигнала ..... 333
11.3. Обнаружение и подавление закладных устройств ..... 339
11.3.1. Демаскирующие признаки закладных устройств ... 339
11.3.2. Методы обнаружения закладных подслушивающих устройств ..... 341
11.3.3. Методы подавления подслушивающих закладных устройств ..... 350
11.3.4. Способы контроля помещений на отсутствие закладных устройств ..... 352
11.4. Методы предотвращения несанкционированной записи речевой информации на диктофон ..... 358
11.5. Методы подавления опасных сигналов акустоэлектрических преобразователей ..... 360
**Глава 12. Экранирование побочных излучений и наводок .... 364**
12.1. Экранирование электромагнитных полей ..... 364
12.2. Экранирование электрических проводов ..... 370
12.3. Компенсация полей ..... 373
12.4. Предотвращение утечки информации по цепям электропитания и заземления ..... 376
**Глава 13. Методы предотвращения утечки информации по вещественному каналу ..... 380**
13.1. Методы защиты информации в отходах производства ..... 380

13.2. Методы защиты демаскирующих веществ в отходах химического производства ..... 383

**Осиовиые положеиия раздела II ..... 385**

**РАЗДЕЛ III. ТЕХНИЧЕСКИЕ ОСНОВЫ ДОБЫВАНИЯ И ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ..... 402**

**Глава 14. Характеристика средств технической разведки ..... 402**

14.1. Структура системы технической разведки ..... 402

14.2. Классификация технических средств добывания информации ..... 404

14.3. Возможности средств технической разведки ..... 411

**Глава 15. Техиические средства подслушиваиия ..... 423**

15.1. Акустические приемники ..... 423

15.2. Диктофоны ..... 439

15.3. Закладные устройства ..... 441

15.4. Лазерные средства подслушивания ..... 451

15.5. Средства высокочастотного навязывания ..... 454

**Глава 16. Средства скрытиого иаблюдеиия ..... 456**

16.1. Средства наблюдения в оптическом диапазоне ..... 456

16.1.1. Оптические системы ..... 459

16.1.2. Визуально-оптические приборы ..... 465

16.1.3. Фото- и киноаппараты ..... 467

16.1.4. Средства телевизионного наблюдения ..... 477

16.2. Средства наблюдения в инфракрасном диапазоне ..... 490

16.3. Средства наблюдения в радиодиапазоне ..... 495

**Глава 17. Средства перехвата сигиалов ..... 502**

17.1. Средства перехвата радиосигналов ..... 502

17.1.1. Антенны ..... 503

17.1.2. Радиоприемники ..... 510

17.1.3. Технические средства анализа сигналов ..... 517

17.1.4. Средства определения координат источников радиосигналов ..... 519
17.2. Средства перехвата оптических и электрических сигналов ..... 521
**Глава 18. Средства добывания информации о радиоактивных веществах ..... 524**
**Глава 19. Система инженерно-технической защиты информации ..... 529**
19.1. Структура системы инженерно-технической защиты информации ..... 529
19.2. Подсистема физической защиты источников информации ..... 532
19.3. Подсистема инженерно-технической защиты информации от ее утечки ..... 548
19.4. Управление силами и средствами системы инженерно-технической защиты информации ..... 552
19.5. Классификация средств инженерно-технической защиты информации ..... 561
**Глава 20. Средства инженерной защиты ..... 564**
20.1. Ограждения территории ..... 564
20.2. Ограждения зданий и помещений ..... 567
20.2.1. Двери и ворота ..... 568
20.2.2. Окна ..... 574
20.3. Металлические шкафы, сейфы и хранилища ..... 577
20.4. Средства систем контроля и управления доступом ..... 580
**Глава 21. Средства технической охраны объектов ..... 591**
21.1. Средства обнаружения злоумышленников и пожара ..... 591
21.1.1. Извещатели ..... 591
21.1.2. Средства контроля и управления средствами охраны ..... 609
21.2. Средства телевизионной охраны ..... 611

21.3. Средства освещения ..... 618
21.4. Средства нейтрализации угроз ..... 620
**Глава 22. Средства противодействия наблюдению ..... 630**
22.1. Средства противодействия наблюдению в оптическом диапазоне ..... 630
22.2. Средства противодействия радиолокационному и гидроакустическому наблюдению ..... 635
**Глава 23. Средства противодействия подслушиванию ..... 641**
23.1. Средства звукоизоляции и звукопоглощения акустического сигнала ..... 641
23.2. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств ..... 654
23.2.1. Классификация средств обнаружения и локализации закладных подслушивающих устройств ..... 654
23.2.2. Аппаратура радиоконтроля ..... 658
23.2.3. Средства контроля телефонных линий и цепей электропитания ..... 664
23.2.4. Технические средства подавления сигналов закладных устройств ..... 667
23.2.5. Нелинейные локаторы ..... 670
23.2.6. Обнаружители пустот, металлодетекторы и рентгеновские аппараты ..... 672
23.2.7. Средства контроля помещений на отсутствие закладных устройств ..... 677
**Глава 24. Средства предотвращения утечки информации через ПЭМИН ..... 686**
24.1. Средства подавления опасных сигналов акустоэлектрических преобразователей ..... 686
24.2. Средства экранирования электромагнитных полей ..... 690
**Основные положения раздела III ..... 696**

**РАЗДЕЛ IV. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ..... 721**

**Глава 25. Организация инженерно-технической защиты информации ..... 721**

25.1. Задачи и структура государственной системы инженерно-технической защиты информации ..... 721

25.2. Организация инженерно-технической защиты информации на предприятиях (в организациях, учреждениях) ..... 734

25.3. Нормативно-правовая база инженерно-технической защиты информации ..... 740

**Глава 26. Типовые меры по инженерно-технической защите информации ..... 749**

26.1. Основные организационные и технические меры по обеспечению инженерно-технической защиты информации ..... 749

26.2. Контроль эффективности инженерно-технической защиты информации ..... 754

**Основные положения раздела IV ..... 760**

**РАЗДЕЛ V. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ..... 765**

**Глава 27. Рекомендации по моделированию системы инженерно-технической защиты информации ..... 765**

27.1. Алгоритм проектирования (совершенствования) системы защиты информации ..... 765

27.2. Моделирование объектов защиты ..... 774

27.3. Моделирование угроз информации ..... 780

27.3.1. Моделирование каналов несанкционированного доступа к информации ..... 781

27.3.2. Моделирование каналов утечки информации ..... 788

27.4. Методические рекомендации по оценке значений показателей моделирования ..... 811

**Глава 28. Методические рекомендации по определению мер инженерно-технической защиты информации ..... 821**

28.1. Общие рекомендации ..... 821

28.2. Методические рекомендации по организации физической защиты источников информации ..... 823

28.2.1. Рекомендации по повышению укрепленности инженерных конструкций ..... 825

28.2.2. Выбор технических средств охраны ..... 826

28.3. Рекомендации по предотвращению утечки информации ..... 835

28.3.1. Типовые меры по защите информации от наблюдения: ..... 835

28.3.2. Типовые меры по защите информации от подслушивания: ..... 837

28.3.3. Типовые меры по защите информации от перехвата ..... 838

28.3.4. Методические рекомендации по «чистке» помещений от закладных устройств ..... 839

28.3.5. Меры по защите информации от утечки по вещественному каналу ..... 847

**Основные положения раздела V ..... 848**

**ЗАКЛЮЧЕНИЕ ..... 857**

**Основные используемые термины и понятия ..... 862**

**Сценарий инженерно-технической защиты информации в кабинете руководителя организации ..... 869**

1.1. Обоснование выбора кабинета как объекта защиты ..... 869

1.2. Характеристика информации, защищаемой в кабинете руководителя ..... 870

1.3. План кабинета как объекта защиты ..... 874

2.1. Моделирование угроз воздействия на источники информации ..... 879
2.2. Моделирование технических каналов утечки информации ..... 880
3.1. Меры по предотвращению проникновения злоумышленника к источникам информации ..... 888
3.2. Защита информации в кабинете руководителя от наблюдения ..... 889
3.3. Меры по защите речевой информации от подслушивания ..... 890
3.4. Предотвращение перехвата радио- и электрических сигналов ..... 892
**ЛИТЕРАТУРА ..... 934**
**Основная литература ..... 934**
**Дополнительная литература ..... 934**

*Учебное издание*
**Торокин Анатолий Алексеевич**

**Инженерно-техническая защита информации**

Заведующая редакцией *Т. А. Денисова*
Корректор *К. Н. Клитина*
Компьютерная верстка *С. Н. Авилкина, О. Ю. Самариной*
Дизайн обложки *Л. А. Смирновой*

Издательство «Гелиос АРВ».
Издательская лицензия ЛР № 066255
107140, г. Москва, Верхняя Красносельская ул., 16.
Тел./факс: (095) 264-44-39, e-mail: info@gelios-arv.ru
Адрес в Internet: http://www.gelios-arv.ru

Формат 60x90/16. Печать офсетная. 60 п. л. Тираж 3000 экз.
Бумага газетная. Заказ № 174

Отпечатано с готовых диапозитивов в
типографии ГП «Облиздат»,
248640, г. Калуга, пл. Старый торг, 5.