ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Кафедра информационных управляющих систем

Н.Н. Мошак

Защищенные информационные системы

Конспект лекций

для специальности 230201 – Информационные системы и технологии

Санкт-Петербург, 2018

Аннотация

В лекционном курсе «**Защищенные информационные системы»** для магистров приводятся общие подходы к обеспечению безопасности информационных систем. Основное внимание уделяется построению информационной безопасности современной корпоративной информационной системе (ИС) на базе архитектуры «клиент-сервер». Описываются модели нарушителей, угрозы информационной безопасности ИС, строится политика информационной безопасности ИС, формулируются требования информационной безопасности, протоколы механизмов защиты и инструментальные средства защиты, комплекс организационно-технических мер по реализации требований и построению системы информационной безопасности, а также организационно-технической схемы контроля состояния информационной безопасности автоматизированной информационной системы организации.

Раздел 1. Безопасность и эволюция архитектур информационных систем

1.1 Понятие информационной безопасности

Информация - самый ценный ресурс в организации, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы. С развитием информационных технологий увеличивается риск утечки информации, заражение вирусами, вмешательства в работу системы.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В ***широком смысле*** информационная безопасность (ИБ) – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность создает условия формирования безопасного состояния информационной среды общества, его использование и развитие в интересах граждан, предприятий и даже государства. Информационная среда — это «сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации». Условно ее можно поделить на три главные предметные составляющие:

- создание и распространение информации;
- создание информационных ресурсов, подготовки информационных продуктов, предоставления информационных услуг;
- потребление информации.

Под информационной безопасностью ***в узком смысле*** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ***неприемлемый ущерб*** субъектам информационных отношений**,** в том числе владельцам и пользователям информации и поддерживающей инфраструктуре, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Информационная безопасность организации основывается на законодательстве Российской Федерации, Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 года, государственных нормативно-методических документах в области информационной безопасности (Государственных стандартах, руководящих документах Федеральной

службы по экспортному и техническому контролю), нормативно-методических документах Мининформсвязи РФ, учитывающих общие принципы обеспечения информационной безопасности, предусматриваемых международными и зарубежными национальными стандартами (такими, как ISO/IEC 17799-2000, ISO/IEC 15408, BS 7799, COBIT и др.).

1.2 Объект и предмет защиты информации

Объектом защиты информации является информационная система (ИС) организации.

Информационная система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели (ЭВМ всех классов и назначений; вычислительные комплексы и системы; вычислительные сети (локальные, региональные и глобальные)).

Предметом защиты в ИС является информация. Целью обеспечения ИБ в ИС организации, является надежное и качественное ее функционирование в условиях возникающих угроз и воздействий, которые могут привести к нарушению и дестабилизации работы ее компонент, в т. ч. и ее подсистемы информационной безопасности.

Информационная безопасность ИС организации – есть заданная вероятность защищенности ее активов (информационное и программное обеспечение, технические средства) с учетом приоритетов услуг защиты, модели угроз и нарушителя. ИС, в которых обеспечивается безопасность информации, называются защищенными.

Информационная безопасность достигается проведением руководством соответствующего уровня ***политики информационной безопасности ИС***. Одноименный документ разрабатывается и принимается как официальный руководящий документ, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в ИС.

На рис. 1. Представлена модель процессов естественных и управляющих воздействий на безопасность ИС. Представленная модель описывает совокупность объективных внешних и внутренних факторов и демонстрирует их влияние на состояние информационной безопасности в организации и на сохранность материальных или информационных ресурсов.

Данная модель включает следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер, влияющие на вероятность реализации угрозы;
- риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования.

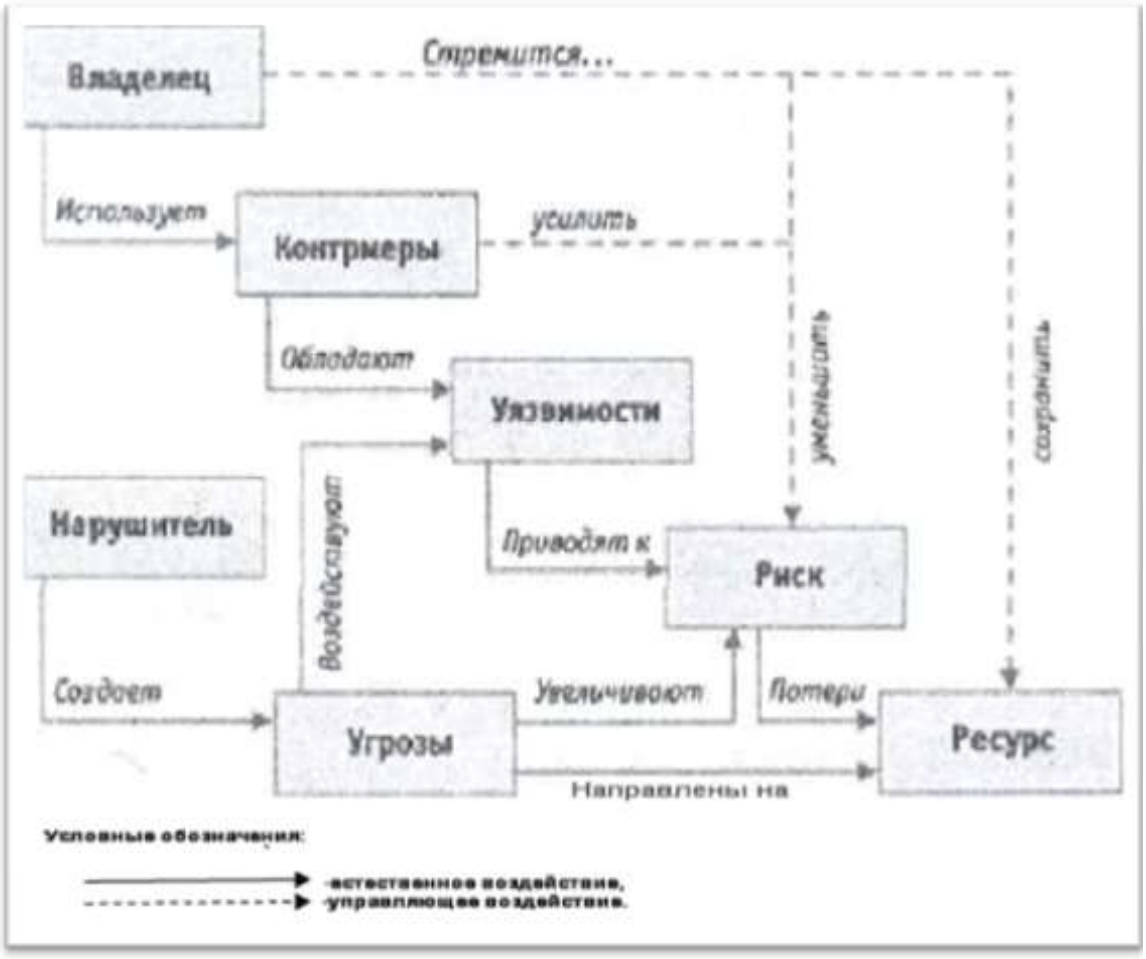

Рис. 1. - Модель процессов естественных и управляющих воздействий на безопасность информационных систем

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности ИС. Цель защиты информации - уменьшение размеров ущерба до допустимых значений.

Под системой защиты информации в ИС понимается единый комплекс правовых норм, организационных и технических мер, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности. Эти меры можно разделить на две группы:

- организационные меры;
- технические меры.

Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами защиты.

Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д.

1.3 Эволюция архитектуры информационных систем

Децентрализация архитектуры первых вычислительных систем стала возможной в связи с появлением персональных компьютеров, к которым мигрировала часть функций центральных ЭВМ. В результате появились распределенные локальные и глобальные вычислительные системы, объединяющие персональные компьютеры и компьютеры, полностью предоставляющие свои ресурсы в общее пользование для других компьютеров сети. Компьютеры, предоставляющие те или иные общие ресурсы, были названы серверами, а компьютеры, использующие общие ресурсы, - клиентами. Соответственно архитектуру таких распределенных вычислительных систем стали называть архитектурой «клиент-сервер» (рис. 1.2). Персональные компьютеры, исполняющие роль клиентов, называют еще рабочими станциями сети.

Рис. 1.2 - Типовая сетевая архитектура «клиент-сервер»

Конкретный сервер характеризуется видом ресурса, которым он владеет. Так, если ресурсом является только база данных, то речь идет о сервере базы данных, назначение которого - обслуживать запросы клиентов, связанные с обработкой данных; если ресурс - это файловая система, то говорят о файловом сервере, или файл-сервере.

Традиционные архитектурные решения ИС основаны на использовании выделенных *файл-серверов или серверов баз данных*. Особенностью серверов баз данных заключается в их способности выполнять специальные запросы к данным. Язык запросов устроен таким образом, что одна команда этого языка может заключать в себе множество элементарных операций над данными. Таким образом можно значительно снизить сетевой трафик, а для увеличения производительности информационной системы потребуется увеличения производительности только сервера баз данных. Кроме этого современные сервера баз данных позволяют хранить на стороне сервера программные модули (хранимые процедуры, триггеры и др.), которые по команде со стороны пользователя (клиента) могут быть запущены на выполнение. В результате, появляется реальная возможность выполнять на стороне сервера не только обработку данных, но и другие действия.

Существуют также варианты архитектур корпоративных информационных систем, базирующихся *на технологии Internet* (Intranet-приложения). Следующая разновидность архитектуры информационной системы основывается *на концепции «хранилища данных» (DataWarehouse) —*

интегрированной информационной среды, включающей разнородные информационные ресурсы. И, наконец, для построения глобальных распределенных информационных приложений используется архитектура интеграции информационно-вычислительных компонентов *на основе объектно-ориентированного подхода.*

Различают несколько моделей архитектуры «клиент-сервер», каждая из которых отражает соответствующее распределение компонентов программного обеспечения между компьютерами сети. Распределяемые программные компоненты выделяют по функциональному признаку.

Функции любого программного приложения могут быть разделены на три группы:

- функции ввода и отображения данных;
- прикладные функции, характерные для предметной области приложения;
- функции накопления информации и управления данными (базами данных, файлами).

Соответственно любое программное приложение можно представить как структуру из трех компонентов:

- компонент представления (presentation), реализующий интерфейс с пользователем;
- прикладной компонент (business application), обеспечивающий выполнение прикладных функций;
- компонент доступа к информационным ресурсам (resource access) или менеджер ресурсов (resource manager), выполняющий накопление информации и управление данными.

Различают несколько моделей архитектуры «клиент-сервер», каждая из которых отражает соответствующее распределение компонентов программного обеспечения между компьютерами сети. Распределяемые программные компоненты выделяют по функциональному признаку. В архитектуре "клиент/сервер" функции приложения распределены между двумя (или более) компьютерами. В соответствии с тем, каким образом это сделано, выделяются три модели архитектуры "клиент/сервер":

1. Модель доступа к удаленным данным (на сервере расположены только данные);
2. Модель сервера управления данными (кроме данных на сервере расположен менеджер информационных ресурсов, например система управления базой данных) - Remote Data Access - RDA;
3. Модель комплексного сервера (на сервере сконцентрированы как данные и менеджер ресурсов, так и прикладной компонент) - DataBase Server - DBS;
4. Модель трехзвенной архитектуры «клиент-сервер» (на одном сервере расположен прикладной компонент, а на другом данные и менеджер ресурсов) - Application Server - AS.

1.3.1. Модель доступа к удаленным данным

В архитектуре «хост/терминал» (рис. 1.3) функции всех трех групп совмещены в одном коде, который выполняется на компьютере-сервере (хосте). Компьютер-клиент в данной архитектуре отсутствует в принципе, а ввод и отображение данных производятся через терминал или компьютер в режиме эмуляции терминала. Приложения обычно разрабатываются на языке четвертого поколения (4GL).

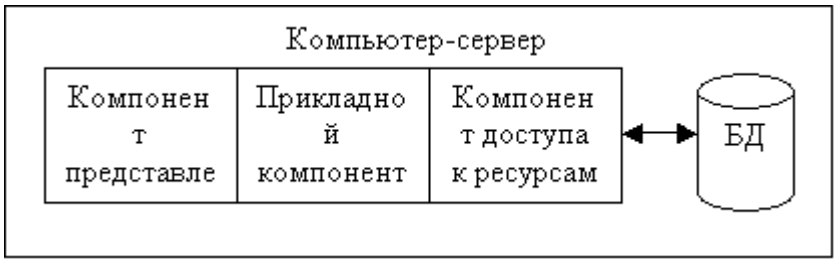

Рис. 1.3 - Модель доступа к удаленным данным

Модель доступа к удаленным данным не обеспечивает высокую производительность, так как вся информация обрабатывается на рабочих станциях, а файлы, содержащие эту информацию, для обработки должны быть переданы по сети с сервера. Преимуществами данной архитектуры являются:

1. Простота разработки приложений.
2. Удобство администрирования и обновления ПО, т. к. все части прикладной системы размещаются на одном компьютере.
3. Низкий трафик, создаваемый в сети, т.к. по сети пересылаются только данные, вводимые пользователем, и данные, отображаемые на экране. Благодаря этому возможна работа по низкоскоростным линиям.
4. Низкая стоимость оборудования рабочих мест. На рабочих местах можно использовать терминалы или дешевые компьютеры с невысокими характеристиками в режиме эмуляции терминала.

К недостаткам можно отнести:

1. Высокие требования ко времени отклика в сети. Несмотря на небольшой объем данных, пересылаемых по сети, время отклика является критичным, т.к. каждый символ, введенный пользователем на терминале, должен быть передан на сервер, обработан приложением и возвращен обратно для вывода на экран терминала.
2. Высокие требования к характеристикам компьютера-сервера, т.к. все пользователи разделяют его ресурсы.
3. Невозможность распределения нагрузки между несколькими компьютерами.
4. Невозможность использования графического интерфейса.

1.3.2. Модель сервера управления данными

В RDA-модели (рис. 1.4) коды компонента представления и прикладного компонента совмещены и выполнятся на компьютере-клиенте. Последний поддерживает как функции ввода и отображения данных, так и прикладные функции ("толстый" клиент).

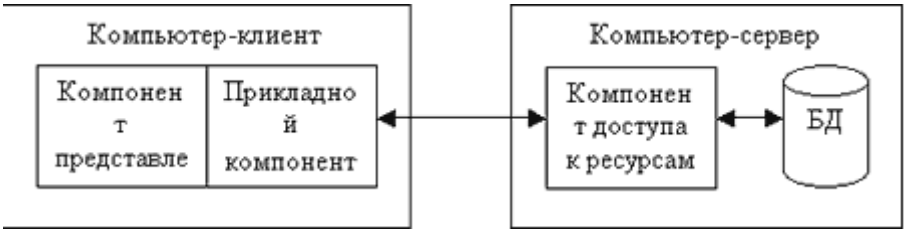

Рис. 1.4. - Модель сервера управления данными

При использовании модели сервера управления данными на сервере, кроме самой информации, расположен менеджер информационных ресурсов, например, система управления базой данных. Компонент представления и прикладной компонент совмещены и выполняются на компьютере-клиенте, который поддерживает как функции ввода и отображения данных, так и чисто прикладные функции. Доступ к информационным ресурсам обеспечивается, как правило, операторами специального языка (например, SQL) или вызовами функций специальной библиотеки (если имеется соответствующий API). Запросы к информационным ресурсам направляются по сети менеджеру ресурсов, например серверу базы данных. Последний обрабатывает запросы и возвращает клиенту блоки данных. Говоря об архитектуре "клиент/сервер", в большинстве случаев имеют в виду именно эту модель.

Главным преимуществом модели сервера управления данными перед моделью доступа к удаленным данным является снижение объема информации, передаваемой по сети, так как выборка требуемых информационных элементов из файлов выполняется не на рабочих станциях, а на сервере. Преимуществом RDA-модели является также широкий выбор средств быстрой разработки приложений (RAD) различных фирм. Кроме того, в настоящее время существует множество инструментальных средств, обеспечивающих быстрое создание приложений с развитым интерфейсом, работающих с SQL-ориентированными СУБД. Большинство из них поддерживают графический интерфейс пользователя в MS Windows, стандарт интерфейса ODBC, содержат средства автоматической генерации кода. Подавляющее большинство этих средств разработки на языках четвертого поколения (включая и средства автоматизации программирования) как раз и создают коды, в которых смешаны прикладные функции и функции представления. Это обеспечивает унификацию и широкий выбор средств разработки приложений.

В то же время RDA-модель имеет ряд недостатков и ограничений.

1. Отсутствие четкого разграничения между компонентом представления и прикладным компонентом, что затрудняет дальнейшее совершенствование ИС, архитектура которой построена на основе данной модели.
2. Очень большая загрузка сети. Приложение является нераспределенным, и вся его логика локализована на компьютере-клиенте, поэтому взаимодействие его с сервером посредством SQL-запросов приводит к передаче по сети данных большого объема, возможно, избыточных. Как только число клиентов возрастает, сеть становится узким местом, ограничивая быстродействие всей информационной системы.
3. Сложность ведения больших проектов. Очевидно, что если различные по своей природе функции (функции представления и чисто прикладные функции) смешаны в одной и той же программе, написанной на языке 4GL, то при необходимости изменения прикладных функций приходится переписывать всю программу целиком. При коллективной работе над проектом, как правило, каждому разработчику поручается реализация отдельных прикладных функций, что делает невозможным контроль за их взаимной непротиворечивостью. Каждому из разработчиков приходится программировать интерфейс с пользователем, что ставит под вопрос единый стиль интерфейса и его целостность.
4. Сложность обновления программного обеспечения, т.к. его замену необходимо производить одновременно на всех компьютерах-клиентах.
5. Низкий уровень безопасности, т.к. реализация разграничения доступа по функциям возможна только на стороне клиента, а на стороне сервера разграничение выполняется только по таблицам базы данных, что снижает защищенность.

1.3.3. Модель комплексного сервера

В DBS-модели (рис. 1.5) процесс, выполняемый на компьютере-клиенте, ограничивается функциями представления ("тонкий" клиент), а прикладные функции реализованы в хранимых процедурах (stored procedure), которые также называют компилируемыми резидентными процедурами, или процедурами базы данных. Они хранятся непосредственно в базе данных и выполняются на компьютере-сервере базы данных, где функционирует и компонент, управляющий доступом к данным, то есть ядро СУБД.

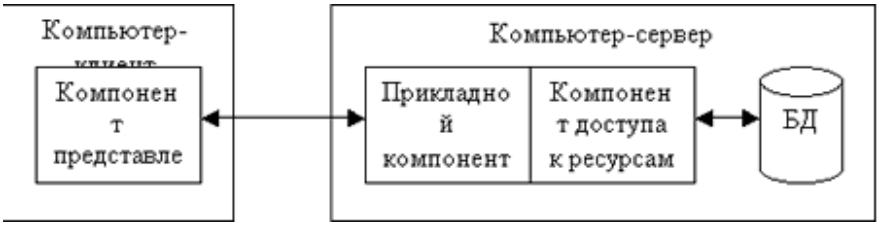

Рис. 1.5 - Модель комплексного сервера

Модель комплексного сервера по сравнению с моделью сервера управления данными является более технологичной. Она строится в предположении, что процесс, выполняемый на компьютере-клиенте, ограничивается функциями представления, в то время как собственно прикладные функции и функции доступа к данным выполняются сервером. DBS-модель реализована в некоторых реляционных СУБД (Ingres, Sybase, Oracle). Ее основу составляет механизм хранимых процедур - средство программирования ядра СУБД. Прикладные функции могут быть реализованы в отдельных программах или в хранимых процедурах, которые называют также процедурами базы данных. Эти процедуры хранятся в словаре базы данных, разделяются между несколькими клиентами и выполняются на том же компьютере-сервере, где функционирует и компонент, управляющий доступом к данным, т. е. ядро СУБД. Язык, на котором разрабатываются хранимые процедуры, представляет собой процедурное расширение языка запросов SQL.

Преимущества DBS-модели очевидны:

1. Более высокая производительность.
2. Возможность централизованного администрирования бизнес-функций, размещенных на сервере.
3. Снижение трафика в сети и соответственно экономия ресурсов сети.
4. Возможность разделения процедуры между несколькими приложениями, и экономия ресурсов компьютера за счет использования единожды созданного плана выполнения процедуры.

Однако есть и недостатки:

1. Средства, используемые для написания хранимых процедур, строго говоря, не являются языками программирования в полном смысле слова. Это разнообразные процедурные расширения SQL, не выдерживающие сравнения по изобразительным средствам и функциональным возможностям с языками третьего поколения (C или Pascal) и тем более четвертого поколения. Они встроены в конкретные СУБД, и, естественно, рамки их использования ограничены. Следовательно, система, в которой прикладной компонент реализован при помощи хранимых процедур, не является мобильной относительно СУБД. В большинстве СУБД отсутствуют возможности отладки и тестирования хранимых процедур, что превращает последние в весьма опасный механизм. Во многих реализациях процедуры являются интерпретируемыми, что делает их выполнение более медленным.
2. Не обеспечивается требуемой эффективности использования вычислительных ресурсов. Объективные ограничения в ядре СУБД не позволяют пока организовать в его рамках эффективный баланс загрузки, миграцию процедур на другие компьютеры-серверы БД и реализовать другие полезные функции. Попытки разработчиков СУБД

предусмотреть в своих системах эти возможности (распределенные хранимые процедуры, запросы с приоритетами и т. д.) пока не позволяют добиться желаемого эффекта.

3. Децентрализация приложений (один из ключевых факторов современных информационных технологий) требует существенного разнообразия вариантов взаимодействия клиента и сервера. При реализации прикладной системы могут понадобиться такие механизмы взаимодействия, как хранимые очереди, асинхронные вызовы и т. д., которые в DBS-модели не поддерживаются.

На практике часто используются смешанные модели, когда поддержка целостности базы данных и некоторые простейшие прикладные функции поддерживаются хранимыми процедурами (DBS-модель), а более сложные функции реализуются непосредственно в прикладной программе, которая выполняется на компьютере-клиенте (RDA-модель).

1.3.4. Модель трехзвенной архитектуры «клиент-сервер»

При существенном усложнении и увеличении прикладного компонента для него может быть выделен отдельный сервер, называемый сервером приложений. В этом случае говорят о **трехзвенной архитектуре** «клиент-сервер», предполагающей наличие трех звеньев: первое звено - компьютер-клиент, второе - сервер приложений, а третье - сервер управления данными. Архитектуру «клиент-сервер», при которой прикладной компонент расположен на рабочей станции вместе с компонентом представления или на сервере вместе с менеджером ресурсов и данными, называют двухзвенной архитектурой.

В AS-модели (рис. 1.6) процесс, выполняющийся на компьютере-клиенте, отвечает, как обычно, за ввод и отображение данных (то есть реализует функции первой группы). Доступ к информационным ресурсам, необходимым для решения прикладных задач, обеспечивается таким же способом, что и в RDA-модели. Серверы приложений выполняются, как правило, на том же компьютере, где функционирует менеджер ресурсов, однако могут выполняться и на других компьютерах.

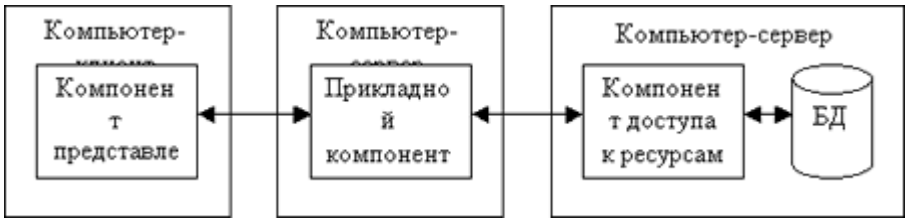

Рис.1.6 - Модель трехзвенной архитектуры «клиент-сервер»

Основным элементом принятой в AS-модели трехзвенной схемы является сервер приложения. В его рамках реализовано несколько прикладных функций, каждая из которых оформлена как служба (service) и предоставляет некоторые услуги всем программам, которые желают и могут

ими воспользоваться. Серверов приложений может быть несколько, и каждый их них предоставляет определенный набор услуг. Любая программа, которая пользуется ими, рассматривается как клиент приложения (Application Client - AC). Детали реализации прикладных функций в сервере приложений полностью скрыты от клиента приложения. AC обращается с запросом к конкретной службе, но не к AS, то есть серверы приложений обезличены и служат лишь своего рода "рамкой" для оформления служб, что позволяет эффективно управлять балансом загрузки. Запросы, поступающие от AC, выстраиваются в очередь к AS-процессу, который извлекает и передает их для обработки службе в соответствии с приоритетами.

Клиент приложения трактуется более широко, чем компонент представления. Он может поддерживать интерфейс с конечным пользователем (в таком случае он является компонентом представления), может обеспечивать поступление данных от некоторых устройств (например, датчиков), может, наконец, быть сервером приложения. Последнее позволяет реализовать прикладную систему, содержащую серверы приложений нескольких уровней.

Архитектура такой системы может выглядеть как ядро, окруженное концентрическими кольцами. Ядро состоит из серверов приложения, в которых реализованы базовые прикладные функции. Кольца символизируют наборы серверов приложения, являющихся клиентами по отношению к серверам внутреннего уровня. Число уровней серверов приложений не ограничено.

Четкое разграничение в архитектуре «клиент-сервер» компонентов программных приложений и рациональное их распределение между компьютерами сети позволяют достичь такого уровня гибкости, который недостижим в одноранговой архитектуре. Благодаря этому обеспечивается высокая эффективность использования компьютерных ресурсов, реализуются возможности расширения и дальнейшего совершенствования вычислительной системы.

AS-модель в наибольшей степени отражает сильные стороны технологии "клиент/сервер":

1. Четкое разграничение логических компонентов приложения.
2. Возможность баланса загрузки между несколькими серверами.
3. Значительное снижение трафика между клиентом и сервером приложений, дающее возможность работы по медленным линиям связи.
4. Высокий уровень защиты данных, т.к. они являются "спрятанными" за сервисами приложения, в которые можно встроить проверку полномочий клиента.
5. Возможность использования в качестве клиентской части приложения стандартного браузера.
6. Упрощение процесса обновления ПО.

Фундаментальное различие между моделями архитектуры "клиент/сервер" заключается в следующем. RDA- и DBS-модели опираются на двухзвенную схему разделения функций. В RDA-модели прикладные функции приданы программе-клиенту, в DBS-модели ответственность за их выполнение берет на себя ядро СУБД. В первом случае прикладной компонент сливается с компонентом представления, во втором - интегрируется в компонент доступа к информационным ресурсам. Напротив, в AS-модели реализована классическая трехзвенная схема разделения функций, где прикладной компонент выделен как важнейший элемент приложения, для его определения используются универсальные механизмы многозадачной операционной системы, и стандартизованы интерфейсы с двумя другими компонентами. Собственно, из этой особенности AS-модели и вытекают ее преимущества.

Классической сетевой архитектуре «клиент-сервер» присущи следующие особенности:

- на сервере порождается не конечная информация, а данные, подлежащие интерпретации компьютерами-клиентами;
- фрагменты прикладной системы распределены между компьютерами сети;
- для обмена данными между клиентами и сервером могут использоваться закрытые протоколы, не совместимые с открытым стандартом TCP/IP, применяемым в сети Интернет;
- каждый из компьютеров сети ориентирован на выполнение только своих локальных программ.

1.3.5. Архитектура «клиент-сервер», основанная на Web-технологии

Многие недостатки, присущие компьютерным сетям с классической архитектурой «клиент-сервер», отсутствуют в вычислительных системах новой архитектуры, которые сконцентрировали и объединили в себе лучшие качества централизованных систем и классических систем «клиент-сервер». Новая архитектура компьютерных сетей была названа интранет-архитектура. Ее часто называют также Web-архитектурой, или архитектурой «клиент-сервер», основанной на Web-технологии. Эта архитектура явилась итогом многолетних исследований и разработок в области приложения глобальных сетевых технологий Интернет к локальным сетям. Появление в 1993 г. архитектуры интранет относят к началу третьего этапа эволюции вычислительных систем.

Основной особенностью архитектуры интранет является возвращение к серверам ряда функций, которые были вынесены за пределы центральной ЭВМ на втором этапе эволюции вычислительных систем. Базисом новой архитектуры является Web-технология, пришедшая из Интернета.

В соответствии с Web-технологией на сервере размещаются так называемые Web-документы, которые визуализируются и интерпретируются программой навигации, функционирующей на рабочей

станции (рис. 1.7). Программу навигации называют еще Web-навигатором, или Web-браузером.

Логически Web-документ представляет собой гипермедийный документ, объединяющий ссылками различные Web-страницы, каждая из которых может содержать ссылки и на другие объекты. Физически Web-документ представляет собой текстовый файл специального формата, содержащий ссылки на другие объекты и Web-документы, расположенные в любом узле сети. Web-документ реально включает только одну Web-страницу, но логически может объединять любое количество таких страниц, принадлежащих различным Web-документам.

Рис.1.7 - Архитектура «клиент-сервер», основанная на Web-технологии

Web-страница, являясь информационным аналогом страницы бумажного носителя, может включать как текст, так и рисунки. Но, в отличие от бумажной страницы, Web-страница может быть связана с компьютерными программами и содержать ссылки на другие объекты. Программа, связанная с Web-страницей, начинает автоматически выполняться при переходе по соответствующей ссылке или открытии Web-страницы. Любые ссылки, включенные в Web-страницу, выделяются другим цветом и/или подчеркиванием. Для перехода по ссылке достаточно щелкнуть по ней мышью.

Получаемая таким образом система гиперссылок основана на том, что некоторые выделенные участки одного документа, которыми могут быть части текста и рисунки, выступают в качестве ссылок на другие логически связанные с ними объекты. При этом объекты, на которые делаются ссылки, могут находиться на любом компьютере сети. В Web-страницу могут быть включены ссылки на следующие объекты:

- другую часть Web-документа;
- другой Web-документ или документ другого формата (например, документ Word или Excel), который может размещаться на любом компьютере сети;

- мультимедийный объект - рисунок, звук, видео;
- программу, которая при переходе на нее по ссылке будет выполняться на сервере;
- программу, которая при переходе на нее по ссылке будет передана с сервера на рабочую станцию для интерпретации или запуска на выполнение навигатором;
- любой другой сервис - электронную почту, копирование файлов с другого компьютера сети, поиск информации и т.д.

Из раскрытого понятия Web-документа становится ясно, что программа навигации, выполняемая на рабочей станции, может не только визуализировать Web-страницы и выполнять переходы к другим объектам, но и активизировать программы на сервере, а также интерпретировать и запускать на выполнение программы, относящиеся к Web-документу, для исполнения на рабочей станции.

Передачу с сервера на рабочую станцию документов и других объектов по запросам, поступающим от навигатора, обеспечивает функционирующая на сервере программа, называемая Web-сервером. Когда Web-навигатору необходимо получить документы или другие объекты от Web-сервера, он отправляет серверу соответствующий запрос. При достаточных правах доступа между сервером и навигатором устанавливается логическое соединение. Далее сервер обрабатывает запрос, передает Web-навигатору результаты обработки, например требуемый Web-документ, и разрывает установленное соединение.

Web-сервер выступает в качестве информационного концентратора, который доставляет информацию из разных источников, а потом однородным образом предоставляет ее пользователю. Навигатор, снабженный универсальным и естественным интерфейсом с человеком, позволяет последнему легко просматривать информацию вне зависимости от ее формата.

Таким образом, в рамках Web-документа может быть выполнена интеграция данных и программных объектов различных типов, расположенных в совершенно разных узлах компьютерной сети. Это позволяет рассредоточивать информацию в соответствии с естественным порядком ее создания и потребления, а также осуществлять единообразный доступ. Приставка Web здесь, а также в названии самой технологии (англ. web - паутина), как раз и отражает тот факт, что работа пользователя осуществляется на основе перехода по ссылкам, которые как нити паутины связывают разнотипные объекты, распределенные по узлам компьютерной сети.

Web-документы, помимо связывания распределенных и разнотипных данных, позволяют рассматривать информацию с нужной степенью детализации, что существенно упрощает анализ больших объемов информации. Можно сосредоточить внимание на главном, а затем изучить выбранный материал в подробностях. Можно эффективно реализовать

многомодельный подход представления материала, создавая различные «взгляды» на требуемую предметную область, отражающие точки зрения той или иной группы сотрудников организации.

Компьютер-клиент, на котором должна выполняться программа навигации, может быть полностью стандартизован. В такой компьютер помимо процессора, основной памяти и монитора достаточно включить небольшой участок внешней памяти, необходимый для хранения и работы программы навигации, а также устройство сопряжения с линией связи. Кроме того, программу навигации можно реализовать аппаратно в специализированном процессоре.

Исходя из изложенного выше можно выделить следующие отличительные черты интранет-архитектуры:

- на сервере порождается конечная информация, предназначенная для представления пользователю программой навигации, а не полуфабрикат, как в системах с классической архитектурой «клиент-сервер»;
- все информационные ресурсы, а также прикладная система сконцентрированы на сервере;
- для обмена данными между клиентами и сервером используются протоколы открытого стандарта TCP/IP, применяемые в Интернете;
- облегчено централизованное управление не только сервером, но и компьютерами-клиентами, так как они стандартизованы с точки зрения программного обеспечения (на каждой рабочей станции достаточно наличия стандартной программы навигации);
- на рабочих станциях помимо своих программ могут выполняться программы с других компьютеров сети.

Предполагается, что перечисленные особенности, за исключением последней, способствуют решению проблемы информационно-компьютерной безопасности.

Концентрация на сервере информации и прикладной системы существенно упрощает построение и администрирование системы безопасности. Использование для обмена данными между компьютерами сети протоколов открытого стандарта TCP/IP приводит к унификации всех способов взаимодействия между рабочими станциями и сервером. Решение по безопасности взаимодействия для одного компьютера и будет стандартным для всех.

Отметим, что важным плюсом использования серверов баз данных является возможность встроить развитую систему безопасности сервера в систему безопасности информационной системы. В частности сервера баз данных позволяют четко разграничить доступ различных пользователей к объектам БД, журналировать все действия производимые пользователем, интегрировать систему безопасности ИС с системой безопасности компьютерной сети и т.д.

1.3.6. Склады данных (DataWarehousing) и системы оперативной аналитической обработки данных

В последние несколько лет все более популярным становится подход, основанный на концепциях склада данных и системы оперативной аналитической обработки данных - OLAP-системы (от On-Line Analitical Processing), т. е. аналитические системы, позволяющие принимать бизнес-решения за счет динамически производимых анализа, моделирования и/или прогнозирования данных. Особенности указанных систем в сравнении с чисто оперативными:

1. Склад данных должен включать как внутренние корпоративные данные, так и внешние данные, характеризующие рынок в целом.
2. Аналитические базы данных имеют объем как минимум на порядок больший, чем оперативные.
3. Склад данных корпорации должен содержать единообразно представленные данные из всех оперативных баз данных. Эта информация должна максимально точно соответствовать текущему содержанию оперативных баз данных и быть согласованной. Отсюда следует необходимость наличия компонента склада данных, извлекающего информацию из оперативных баз данных и "очищающего" эту информацию.
4. Оперативные информационные системы проектируются и разрабатываются в расчете на решение конкретных задач. Обычно набор запросов к оперативной базе данных становится известным уже на этапе проектирования системы. Набор запросов к аналитической базе данных предсказать невозможно. Склады данных для того и существуют, чтобы отвечать на неожиданные (ad hoc) запросы аналитиков. Можно рассчитывать только на то, что запросы будут поступать не слишком часто и затрагивать большие объемы информации. Размеры аналитической базы данных стимулируют использование запросов с агрегатами (сумма, минимальное, максимальное, среднее значение и т.д.).
5. Оперативные базы данных по своей природе являются сильно изменчивыми. Это учитывается в используемых СУБД. Аналитические базы данных меняются только тогда, когда в них загружается оперативная или внешняя информация, в результате оказывается разумным использовать другие, более быстрые при выполнении операций массовой выборки методы индексации, поддерживать упорядоченность информационных массивов, сохранять заранее вычисленные значения агрегатных функций и т.д.
6. Если для оперативных информационных систем обычно хватает защиты информации на уровне таблиц (по правилам SQL-ориентированных баз данных), то информация аналитических баз данных для ее защиты требуются более тонкие приемы (например, при использовании реляционных баз данных установка

индивидуальных привилегий доступа для индивидуальных строк и/или столбцов таблицы).

С учетом приведенных замечаний общая архитектура склада данных и системы аналитической обработки данных может выглядеть так, как показано на рис. 1.8.

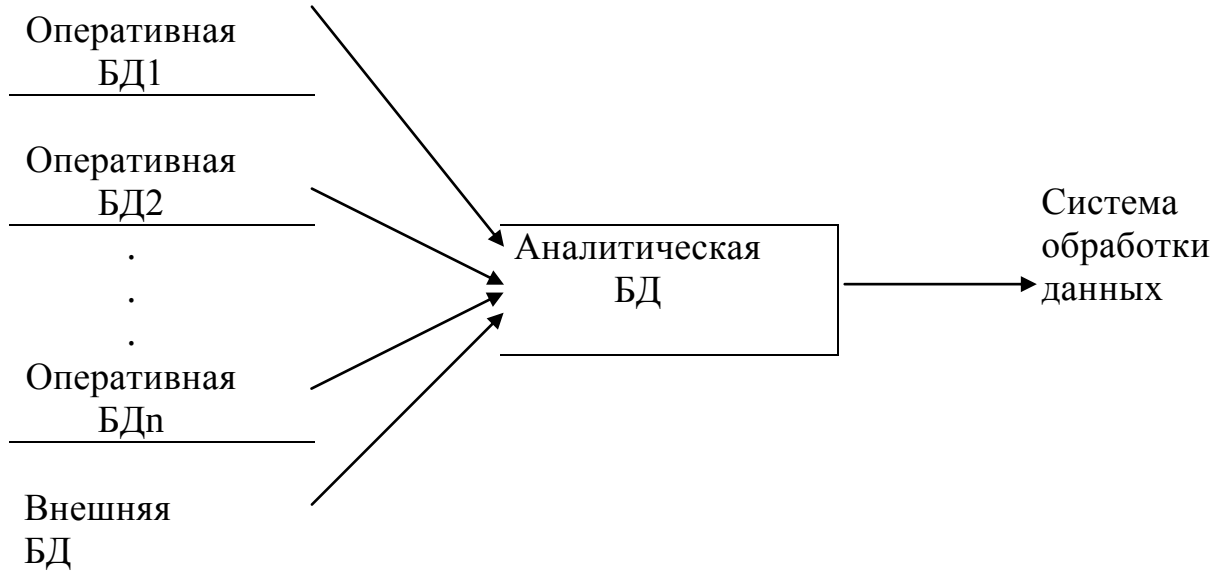

Рис. 1.8 - Схематическое представление архитектуры склада данных и системы аналитической обработки данных

1.3.7. Интегрированные распределенные приложения

На практике по разным причинам возникают потребности в интеграции независимо и по-разному организованных информационно-вычислительных ресурсов. При этом интегрировать приходится неоднородные БД, распределенные в вычислительной сети. Это в значительной степени усложняет реализацию. Дополнительно к собственным проблемам интеграции приходится решать все проблемы, присущие распределенным СУБД: управление глобальными транзакциями, сетевую оптимизацию запросов и т. д. Как правило, для внешнего представления интегрированных и мульти-БД используется (иногда расширенная) реляционная модель данных, последнее время все чаще предлагается использовать объектно-ориентированные модели, но на практике пока основой является реляционная модель. Поэтому, в частности, включение в интегрированную систему локальной реляционной СУБД существенно проще и эффективнее, чем включение СУБД, основанной на другой модели данных. Основным недостатком систем интеграции неоднородных баз данных является то, что при этом не учитываются "поведенческие" аспекты компонентов прикладной системы. Легко заметить, что даже при наличии развитой интеграционной системы, большинство из указанных выше проблем не решается.

Естественным развитием взглядов на информационные ресурсы является их представление в виде набора типизированных объектов, сочетающих возможности сохранения информации (своего состояния) обработки этой информации (за счет наличия хорошо определенного множества методов, применимых к объекту). Наиболее существенный вклад в создание соответствующей технологии внес международный консорциум OMG (Object Management Group), выпустивший ряд документов, в которых специфицируются архитектура и инструментальные средства поддержки распределенных информационных систем, интегрированных на основе общего объектно-ориентированного подхода. В базовом документе специфицируется эталонная модель архитектуры (Object Management Architecture, OMA) распределенной информационной системы (рисунок 1.9).

Рис. 1.9 - Эталонная модель OMA

Согласованная с архитектурой OMA прикладная информационная система представляется как совокупность классов и экземпляров объектов, которые взаимодействуют при поддержке брокера объектных заявок (ORB - Object Request Broker). ORB. Общие средства (Common Facilities) и объектные службы (Object Services) относятся к категории промежуточного программного обеспечения (middleware) и должны поставляться вместе. Объектные службы представляют собой набор услуг (интерфейсов и объектов), которые обеспечивают выполнение базовых функций, требуемых для реализации прикладных объектов и объектов категории "общие средства" (например, специфицированы служба именования объектов, служба долговременного хранения объектов, служба управления транзакциями и т. д.). Общие средства содержат набор классов и экземпляров объектов, поддерживающих функции, полезные в разных прикладных областях (например, средства поддержки пользовательского интерфейса, средства управления информацией и т. д.).

В основе OMA лежит базовая объектная модель (Core Object Model, COM), в которой специфицированы такие понятия, как объект, операция, тип, подтипизация, наследование, интерфейс. Определены также способы согласованного расширения COM в разных объектных службах.

Интерфейсы объекта-клиента и объекта-сервера .должны быть определены на специальном языке (Interface Definition Language, IDL), который очень напоминает компонент спецификации класса (без реализации) языка Си++. Обращения к ORB могут быть сгенерированы статически при компиляции спецификаций IDL или выполнены динамически с использованием специфицированного в документах OMG API брокера объектных заявок. Правила построения и использования ORB определены в документе OMG CORBA (Common Object Request Broker Architecture).

Отметим, что проблемы интеграции неоднородных информационных ресурсов являются актуальными для корпораций и существуют технологии, позволяющие решать эти проблемы.

Контрольные вопросы по разделу 1

Раздел 2. Построение политики информационной безопасности информационных систем

В основе безопасности организации и в первую очередь безопасности ее ИС лежит политика информационной безопасности (далее – «ПИБ» ИС). В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению информационной безопасности ИС организации. В узком — как локальный нормативный документ, определяющий требования безопасности, систему мер либо порядок действий, а также ответственность сотрудников и механизмы контроля для определенной области обеспечения информационной безопасности.

Под политикой информационной безопасности ИС понимается формальная спецификация правил и рекомендаций, требований и руководящих принципов в области ИБ, которыми руководствуются хозяйствующие субъекты организации в своей деятельности и на основе которых пользователи ИС используют, накапливают и распоряжаются информационными ресурсами и технологическими ценностями. ПИБ ИС организации является основополагающим документом, определяющим систему приоритетов, принципов и методов достижения целей обеспечения защищенности активов ИС организации в условиях наличия угроз.

Основные этапы построения политики информационной безопасности ИС включают в себя:

- описание объекта защиты;
- определение основных приоритетов информационной безопасности;
- проведение анализа рисков. Формирование перечня критичных ресурсов, нуждающихся в защите, по результатам проведения анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для предприятия.
- определение модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;
- определение модели угроз информационной безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя;
- определение перечня требований информационной безопасности ИС, определяемых по результатам анализа рисков;
- разработка комплекса организационных и программно-технических мер по реализации требований ИБ ИС и построению подсистемы информационной безопасности (ПИБ) ИС;
- разработка организационно-технической схемы контроля состояния информационной безопасности ИС.

Формирование требований к ИБ ИС организации, позволяющих уменьшить риски информационной безопасности до приемлемой величины, является одним из заключительных этапов построения Политики. Указанные требования лежат в основе построения ПИБ ИС организации, которая является неотъемлемым элементом системы управления ИС и реализует цели и задачи ее политики ИБ.

Требования политики ИБ ИС организации обеспечиваются на основе согласованного комплекса мер и средств, реализуемых ПИБ, в том числе: административных и организационно-технических норм и регламентов, механизмов защиты, программно-технических средств защиты, а также регулярного электронного мониторинга ее состояния. Для обеспечения поддержки и эффективного использования механизмов защиты ПИБ ИС организации должна содержать функцию управления защитой. Управление защитой осуществляется для обеспечения контроля функционирования средств и механизмов защиты, а также для контроля состояния ИБ ИС в целом.

2.1. Описание объекта защиты

Информационная система организации представляет собой совокупность территориально разнесенных объектов, информационный обмен между которыми осуществляется посредством использования открытых каналов связи, предоставленных сторонними операторами электросвязи.

ИС предназначена для обеспечения работоспособности информационной инфраструктуры организации, предоставления сотрудникам структурных подразделений различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов. Перечислим основные особенности распределенной ИС:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;
- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки
- информации большого количества пользователей и персонала различных категорий;

- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения.

Современные ИС строятся, как правило, на архитектуре «клиент-сервер» с применением технологии виртуальных серверов и предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищенности, обрабатывается конфиденциальная информация с различным грифом секретности, а в «открытом» контуре - открытая информация. При этом сертифицированными средствами однонаправленной передачи информации обеспечивается только односторонняя передача информации из «открытого» контура в «закрытый». Типовая схема организации взаимодействия контуров ИС приведена на рис. 2.1. Вешнее взаимодействие ИС с корпоративными системами осуществляется через «закрытый» контур с применением сертифицированных средств криптографической защиты информации (СКЗИ) с шифрованием информации, а с другими системами – через «открытый» контур с применением сертифицированных межсетевых экранов (МЭ).

В качестве базового сетевого протокола используется IP-протокол

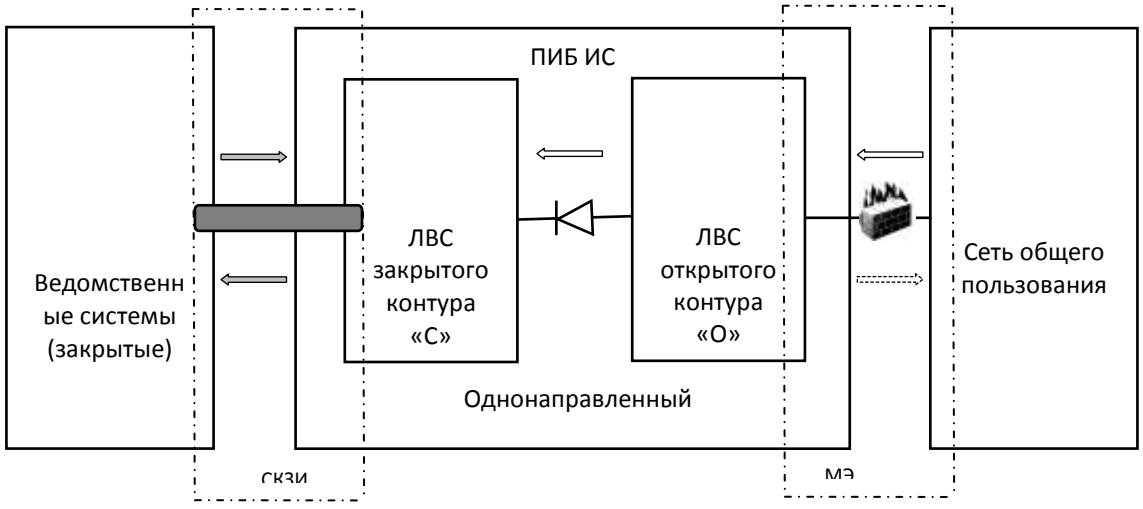

Рис. 2.1 - Обобщенная схема информационных потоков в ИС

В общем случае корпоративная ИС организации на технологии «клиент-сервер» включает в себя следующие функциональные компоненты:

- сервера СУБД и файл-сервера, осуществляющие обработку и хранение информации;

- автоматизированные рабочие места (АРМ) пользователей ИС;
- корпоративная мультисервисная сеть связи на основе IP-QoS технологий, включающая в себя локальную вычислительную сеть (ЛВС) и WAN-компоненту, обеспечивающую связь территориально удаленных ЛВС организации. В корпоративную сеть входят структурированные кабельные системы (СКС), на базе которых строятся ЛВС, сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.) и внешние каналы связи.

2.1.1. Виды информационных ресурсов, хранимых и обрабатываемых в системе

В ИС организации хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации. К конфиденциальной и служебной информации, циркулирующей в ИС, относятся:

- персональные данные сотрудников организации и партнеров, хранимые в БД и передаваемые по сети;
- сообщения электронной почты и информация БД, содержащие служебные сведения, информацию о деятельности организации и т.п.;
- конструкторская и технологическая документация, перспективные планы развития, модернизации производства, реализации продукции и другие сведения, составляющие научно-техническую и технологическую информацию, связанную с деятельностью организации;
- финансовая документация, бухгалтерская отчетность, аналитические материалы исследований о конкурентах и эффективности работы на финансовых рынках;
- другие сведения, составляющие деловую информацию о внутренней деятельности организации.

К строго конфиденциальной информации, которая потенциально может циркулировать в ИС, относятся сведения стратегического характера, разглашение которых может привести к срыву выполнения функций организации, прямо влияющих на его жизнедеятельность и развитие, нанести невосполнимый ущерб деятельности и престижу организации, сорвать решение стратегических задач, проводимой ей политики и, в конечном счете, привести к ее краху.

К категории открытой относится вся прочая информация, не относящаяся к конфиденциальной.

2.1.2. Структура информационных потоков

Внутренние информационные потоки

Внутри ИС выделяются следующие информационные потоки:

- передача файлов между файловыми серверами и пользовательскими АРМ;

- передача сообщений электронной почты;
- передача юридической и справочной информации между серверами БД и АРМ;
- деловая переписка;
- Передача отчетной информации;
- передача бухгалтерской информации между АРМ и сервером БД в рамках автоматизированных систем «1С Бухгалтерия», «1С Зарплата и Кадры», «Оперативный учет».

Внешние информационные потоки

В качестве внешних информационных потоков используются:

- передача отчетных документов (производственные данные) от филиалов организации, по каналам корпоративной сети, а также с использованием магнитных носителей.
- передача финансовых и статистических отчетных документов от филиалов организации;
- внутриведомственный и межведомственный обмен электронной почтой;
- передача информации по коммутируемым каналам удаленным пользователям.
- различные виды информационных обменов между ИС и сетью Интернет.

Подсистема информационной безопасности «закрытого» контура должна обеспечивать:

- сохранение информации в тайне, включая защиту информации от утечки по техническим каналам;
- защиту информации от несанкционированного доступа (далее - НСД) в соответствии с требованиями соответствующего класса защищенности с учетом актуальных угроз безопасности информации «закрытого» контура;
- идентификацию и аутентификацию;
- аудит (регистрацию событий);
- контроль целостности;
- администрирование;
- однонаправленную передачу данных;
- шифрование данных;
- антивирусную защиту.

Подсистема информационной безопасности «открытого» контура должна обеспечивать:

- защиту информации от НСД с учетом актуальных угроз безопасности информации «открытого» контура, отраженных в модели нарушителя;
- защиту информации, передаваемой между «открытыми» контурами объектов разного уровня по открытым каналам, включая Интернет;

- администрирование;
- антивирусную защиту;
- межсетевое экранирование.

2.2. Определение основных приоритетов информационной безопасности ИС

2.2.1. Базовые услуги безопасности

Стандарт ГОСТ Р ИСО 7498-2-99 определяет пять базовых услуг для обеспечения безопасности (защиты) компьютерных систем и сетей: конфиденциальность (Confidentiality), аутентификация (Authentication), целостность (Integrity), Контроль доступа (Access Control), причастность Nonrepudiation), входящие в архитектуру защиты ЭМ, и механизмы, обеспечивающие функционирование этих услуг. Для всех этих услуг определены также варианты, как например, для коммуникаций с установлением соединения и без установления соединения, или обеспечения безопасности на уровнях коммуникации, пакетов или отдельных полей. Этот набор услуг не является единственно возможным, однако он является общепринятым. В данном разделе описаны услуги и варианты их реализации, а также их соотношение между собой и к модели ВОС.

Конфиденциальность

В стандарте ГОСТ Р ИСО 7498-2-99 конфиденциальность определена как "свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных (неуполномоченных) личностей, обьектов или процессов". Вопросам обеспечения конфиденциальности уделяется наибольшее внимание в системах, где раскрытие информации возможно во многих точках по пути передачи.

Для этой услуги определяется четыре версии: для систем с установлением связи; для систем без установления связи; защита отдельных информационных полей; защита от контроля трафика. Первые две версии относятся к соответствующим протоколам с установлением или без установления связи. Конфиденциальность с установлением связи может быть обеспечена на любом уровне, кроме Сеансового или Представительного. Это согласуется с моделью ВОС, где коммуникационные услуги предлагаются на всех уровнях. Конфиденциальность без установления связи может реализовываться на всех уровнях, кроме Физического, Сеансового и Представительного, причем Физический уровень исключен потому, что он по своей природе требует установления связи.

Третья версия конфиденциальных услуг, предназначенных для защиты отдельных информационных полей, используется для обеих типов сетей (с установлением связи и без) и требует, чтобы только отдельные поля в пакетах были защищены. Эта услуга предлагается только для Прикладного

уровня, где необходимое поле может иметь другой способ кодирования, чем обеспечивает стандартный протокол.
Защита от контроля трафика должна предотвращать возмождность анализа и контроля трафика. Это достигается за счет кодирования информации об источнике-назначении, количестве передаваемых данных и частоты передачи. Эти внешние характеристики могут быть доступны для злоумышленника, даже если пользовательские данные будут защищены. Например, легко различить трафик Telnet и FTP в зависимости от размера пакетов, даже если информация о порте сервиса и данных выше уровня IP будут защищены. Наиболее легко данная услуга реализуется на физическом уровне, но отдельные компоненты данной услуги могут предлагаться и на Сетевом и Прикладном уровнях. В этом плане естественную большую защищенность имеет широко внедряющаяся сейчас технология ATM (Asynchronous Transfer Mode), которая обеспечивает фиксированный размер пакетов и стандартную инкапсуляцию пакетов протоколов различного уровня.

Аутентификация

В стандарте ГОСТ Р ИСО 7498-2-99 определяется два типа услуг аутентификации: достоверность происхождения (источника) данных и достоверность собственно источника соединения или объекта коммуникации (peer-entity).
Достоверность источника данных предполагает подтверждение того, что "источник полученных данных именно тот, который указан или обьявлен". Эта услуга существенна для коммуникации без установления связи, при которой каждый пакет является независимым от других, и единственное, что может быть гарантировано с точки зрения аутентификации - это то, что источник пакета именно тот, который указан в заголовке пакета. Эта услуга очень близка к обеспечению целостности данных в сетях без установления связи, когда установление подлинности источника не очень существенно, если нарушена целостность данных.

В системах с установлением связи, аутентификация объекта коммуникаций является необходимой функцией, определенной как "подтверждение того, что объект коммуникации при соединении именно тот который объявлен". Эта форма аутентификации подразумевает установление своевременности или фактора времени за счет включению идентификации объекта коммуникации для конкретного случая соединения, которые недостижимы при помощи простой проверки происхождения данных. Т.о., атака, использующая воспроизведение данных, связанных с другим сеансом связи, даже между теми же объектами коммуникации, может быть нарушена/предотвращена, благодаря использованию этой услуги.

Обе формы аутентификации определены для Сетевого, Транспортного и Прикладного уровней, на которых реализуются протоколы с установлением связи и без установления связи.

Целостность

Согласно стандарта ГОСТ Р ИСО 7498-2-99 целостность имеет две базовые реализации: для сетей с установлением связи и без установления связи, каждая из которых может применяться для избранных групп информационных полей. Однако услуги защиты целостности в сетях с установлением связи могут дополнительно включать функции восстановления данных в случае, если нарушена их целостность. Таким образом, обеспечение целостности данных в сетях с установлением связи предполагает обнаружение "любой модификации, включения, удаления, или повторной передачи данных в последовательности (пакетов)". Использование услуг обеспечения целостности данных в сетях с установлением связи совместно с идентификацией объекта коммуникаций (peer-entity) позволяет достичь высокой степени защищенности. Эта услуга используется на уровнях Сетевом, Транспортном и Прикладном, при этом средства восстановления данных возможны только на двух верхних уровнях.

Целостность в сетях без установления связи ориентирована на определение модификаций каждого пакета, без анализа большего обьема информации, например, сеанса или цикла передачи. Таким образом, эта услуга не предотвращает умышленное удаление, включение или повторную передачу пакетов и является естественным дополнением аутентификации источника данных. Эта услуга также доступна на уровнях Сетевом, Транспортном и Прикладном. Здесь также возможно применение протокола IEEE802.10 SDE для обеспечения целостности на уровне данных при коммуникации без установления связи.

Контроль доступа

В стандарте ГОСТ Р ИСО 7498-2-99 контроль доступа определен как "предотвращение неавторизованного использования ресурсов, включая предотвращение использования ресурсов недопустимым способом". Т.е. данная услуга не только обеспечивает доступ только авторизованных пользователей (и процессов), но и гарантирует только указанные права доступа для авторизованных пользователей. Таким образом эта услуга предотвращает неавторизованный доступ как "внутренних", так и "внешних" пользователей.

Контроль доступа часто путается с аутентификацией и конфиденциальностью, но на самом деле эта услуга с предоставляет более широкие возможности. Услуга контроля доступа используется для установления политики контроля/ограничения доступа. Политика контроля доступа (или авторизации) согласно ГОСТ Р ИСО 7498-2-99 устанавливается в двух измерениях: критерии для принятия решения о доступе и средства, при помощи которых регулируется контроль. Два типа политики доступа в зависимости от используемых критериев принятия решения могут быть основаны на идентичности явлений и объектов (identity-

based) или на правилах (последовательности) доступа (rule-based). Первый тип политики контроля доступа основан на использовании услуги аутентификации для проверки идентичности субъекта доступа (пользователя, процесса, промежуточной или конечной системы, или сети) прежде, чем предоставить им доступ к ресурсам. Форма идентичности зависит от различия и типа аутентификации для различных уровней, на которых эта услуга обеспечивается. Так, например, пользователь и процесс является объектом контроля доступа на Прикладном уровне, но не на Сетевом уровне.

Политика, использующая регламентированные правила доступа, предполагает принятие решения о доступе на основе последовательности правил, которые соотносят аутентификацию с точностью. Например, правила могут быть выражены в терминах времени и даты доступа или "благонадежности", которую имеет данный пользователь.

Услуга контроля доступа может использоваться на уровнях Сетевом, Транспортном и Прикладном.

Причастность ("неотпирательство")

Данная услуга относится только к Прикладному уровню и, обычно, широко не обсуждается. В стандарте ГОСТ Р ИСО 7498-2-99 причастность определяется, как "предотвращение возможности отказа одним из реальных участников коммуникаций от факта его полного или частичного участия в передаче данных". Две формы причастности определены: причастность к посылке сообщения и подтверждение (доказательство) получения сообщения.

Первая форма данной услуги предоставляет получателю доказательства, что сообщение было послано источником и его целостность не нарушена, на случай отказа отправителя от этого факта. Вторая форма причастности предоставляет источнику доказательства того, что данные были получены получателем, в случае попыток последнего отказаться от этого факта. Обе формы являются более мощными по сравнению с аутентификацией происхождения данных. Отличием здесь является то, что получатель или отправитель данных может доказать третьей стороне факт посылки (получения) данных и невмешательства посторонних. Основными объектами реализации данных сервисов являются протоколы обмена данными, как например, Electronic Data Interchange.

Доступность

Доступность может быть определена как дополнительная услуга обеспечения защищенности сетей. Доступность, как одна из услуг обеспечения безопасности, может быть предметом атаки с целью сделать ресурсы или сервисы компьютерной системы недоступными (или сделать их "качество" неудовлетворительным) для пользователя.

Доступность может быть характеристикой качества данного ресурса или услуги, или, частично, определяться услугой контроля доступа. Однако

характер атак с целью ограничения доступа пользователя и средства борьбы с ними не относиться к собственно услугам и ресурсам или не обеспечиваются услугами контроля доступа. Поэтому целесообразно выделение отдельно услуги обеспечения доступности, который должен реализовываться специальными механизмами на Сетевом уровне (как например, возможность использования альтернативного пути при атаке на доступную полосу основного канала) или Прикладном уровне.

Для реализации базовых услуг безопасности в сети могут применяться как *специальные механизмы защиты* («Шифрование», «Заполнение трафика», «Управление маршрутизацией», «Цифровая подпись», «Контроль доступа», «Обеспечение целостности», «Аутентификация», «Нотаризация»), так и *общие механизмы защиты* («Доверительная функциональность», «Метки безопасности», «Аудиторская проверка»), которые могут быть задействованы для усиления последних. На практике услуги безопасности должны быть включены в соответствующие уровни логической структуры сети для обеспечения требований ее политики ИБ.

2.2.2. Специальные механизмы обеспечения безопасности

Стандарт ГОСТ Р ИСО 7498-2-99 содержит краткое описание механизмов обеспечения безопасности и таблицу возможного соотнесения их к уровням модели ВОС и услугам. При этом не рассматриваются вопросы обеспечения безопасности сетей на Физическом уровне, включая средства контроля электромагнитного излучения систем обработки информации, что является важной задачей обеспечения безопасности информации в национальном понимании.

Выделяются специальные механизмы обеспечения безопасности, которые используются для обеспечения специфических услуг и отличаются для различных услуг, и общие, не относящиеся к конкретным услугам. Ниже дано краткое описание специальных механизмов безопасности, а в таблице 1 приведена существующая связь между услугами безопасности и этими механизмами.

Шифрование

Шифрование (Encipherment, в отличие от Encryption) предполагает использование криптографии для преобразование данных, чтобы сделать их нечитаемыми или неосмысленными. Шифрование (кодирование) обычно применяется совместно с комплементарной функцией - дешифрованием (декодированием). Используется шифрование с симметричными ("закрытыми") ключами (secret key) или несимметричными ("открытыми") ключами (public key).

Шифрование обычно используете для обеспечения конфиденциальности, но может также поддерживать другие услуги безопасности. Такая возможность существует потому, что любое изменение

закодированного текста (шифрограммы) приводит к непредсказуемым изменим исходного текста. При использовании шифрования можно также реализовать механизмы обеспечения целостности и аутентификации для того же уровня или для более высоких уровней. Задача генерации, хранения и распространения криптографических ключей является отдельной задачей управления безопасностью систем.

Заполнение трафика

Заполнение трафика применяется для обеспечения конфиденциальности трафика (потока) информации для уровней, выше Физического (в частности, на Сетевом и Прикладном уровнях). Заполнение трафика может включать генерацию случайного трафика, заполнение дополнительной информацией информативных пакетов, передача пакетов через промежуточные станции или в "ненужном" направлении. Оба типа пакетов, как информативный, так и случайный, могут дополняться до постоянной или случайной длины.

Управление маршрутизацией

Управление маршрутизацией применяется для обеспечения конфиденциальности на Сетевом и Прикладном уровнях с целью предотвращения контроля пути следования данных от Отправителя (источника) до Получателя (приемника). Выбор пути может производиться конечной системой (source routing - маршрутизация, определяемая источником) или выполняться промежеточной системой, основываясь на использовании меток безопасности, вводимых в пакет конечной системой. Этот механизм требует специальной надежности (доверительности) промежуточных систем и может иметь существенные вариации при использовании различных промежуточных систем. Этот механизм может также использоваться для обеспечения целостности с функциями восстановления для выбора альтернативных путей в случаях возникновения атак, приводящих к прерыванию коммуникаций.

Цифровая подпись

Использование цифровой подписи является достаточно распространенным механизмом обеспечения безопасности. Цифровая подпись обычно использует открытые ключи, генерируется отправителем данных и проверяется получателем. Несимметричная криптография может использоваться для шифрования котрольной суммы подписываемого сообщения при помощи "закрытой" части ключа посылателя и в последующем дешифроваться получателем при помощи "открытой" части ключа отправителя.

Использование открытых ключей для цифровой подписи служит для подтверждения происхождения сообщения, но не контролирует получателя сообщения. Этот механизм используется для обеспечения услуг

аутентификации и целостности, для которых субъект верификации подписанных данных заранее неизвестен. При определенном выборе контролируемого параметра цифровая подпись также может применяться для обеспечения услуги причастности.

Механизмы обеспечения контроля доступа

Механизмы обеспечения контроля доступа используются для обеспечения услуг контроля доступа. Большинство этих механизмов пришло из практики безопасности компьютерных систем и часто относиться к вопросам обеспечения политики контроля доступа. Например, для поддержки политики доступа на основе идентификации объекта доступа используется специальная база данных, которая определяет права доступа к ресурсам для отдельных обьектов доступа. Другим вариантом данного механизма может быть использование специального маркера "полномочий" для определения текущих прав доступа к имеющимся ресурсам.

Многие механизмы контроля доступа используют механизмы аутентификации для идентификации объекта доступа, или используют "метки безопасности" в случае применяя политики доступа на основе правил. Политика доступа на основе правил может использовать также другие данные - время и дату, последовательность (путь) доступа и др..

Механизмы обеспечения целостности данных

Целостность отдельного пакета может быть обеспечена добавление к нему контрольной величины, которая является функцией содержащихся в пакете данных. Контрольная величина может вычисляться с использованием шифрования или без него. Если контрольная величина вычисляется на уровне, где применяется шифрование, или выше, механизмы этого типа могут быть также использованы как для подтверждения целостности данных в системах без установления связи, так и для аутентификации источника данных. Обычно для этих целей используются симметричные ключи (известные только для посылателя и получателя информации). Применение несимметричных ключей требует большего времени расчетов и поэтому считается неэффективным.

Для обеспечения целостности последовательности пакетов в протоколах с установлением связи одновременно с контрольными величинами отдельных пакетов используются обычные средства протоколов с установлением связи - нумерация пакетов, повторная передача, удаление пакетов, а также дополнительные средства - временные или синхронизирующие метки, обычно используемые для таких применений, как цифровые видео или аудио приложения.

Механизмы аутентификации

Как было сказано выше аутентификация источника (происхождения) данных часто обеспечивается использованием механизма целостности

совместно с шифрованием. Для широковещательных применений такие же функции может обеспечить цифровая подпись. Логическая аутентификация пользователя компьютерной системы выполняется на основе пароля.

Аутентификация объекта коммуникации обычно выполняется посредством двойного или тройного подтверждения связи («рукопожатия»), аналогичного механизмам синхронизации нумерации последовательности пакетов в протоколах с установлением связи. Односторонний (однократный) обмен обеспечивкает только однократный аутентификацию и не может гарантировать своевременность обмена. Двухсторонний (двукратный) обмен обеспечивает взаимную аутентификацию источника и приемника, но не обеспечивает своевременность обмена без специальных средств синхронизации. Троекратный обмен позволяет достичь полной взаимной аутентификации систем без дополнительной синхронизации. Тут также аутентификация использует специальные механизмы управления криптографическими ключами. Вариант одно-, двух- или трехстороннего обмена для аутентификации источника и приемника реализован в стандарте распределенной службы директорий X.500 (в частности, X.509). При одно- и двукратном обмене аутентификационными сообщениями обычно используются временные метки, но для распределенных приложений синхронизация системных времен является проблемой.

Нотаризация (заверение)

Механизмы нотаризации (заверения) используют третью сторону, пользующуюся доверием двух общающихся субъектов, для обеспечения подтверждения характеристик передаваемых данных. Наиболее часто механизм нотаризации применяется для обеспечения услуги причастности. В частности, нотаризация может применяться совместно с цифровой подписью на основе открытого ключа для подтверждения причастности отправителя данных. Использование нотаризации позволяет включить параметр времени для обеспечения достоверности механизма.

Нотаризация может также применяться для обеспечения надежной временной метки, обеспечиваемой "временным нотариусом". Такая метка может содержать цифровую подпись "нотариуса", идентификатор (кодированный) сообщения, имя отправителя и получателя, а также зарегистрированные время и дату получения сообщения. При этом "нотариус" не имеет доступа к самому сообщению, соблюдая его конфиденциальность.

В таблице 2.1 приведена возможная реализация услуг безопасности отдельными специальными механизмами защиты или их сочетанием. Организация защищенного сеанса связи с установлением соединения предусматривает запрос/подтверждение услуг безопасности на фазе установления защищенного соединения. Если служба безопасности определяется в качестве факультативно предусматриваемой отдельным уровнем, это означает, что она реализуется определенными механизмами

защиты, работающими в рамках этого уровня, если иное не оговорено. При этом механизм защиты может включаться в процесс обслуживания протокольного блока уровня для каждого типа информации и/или представлять собой отдельную услугу уровня.

Таблица 2.1. - Реализация базовых услуг безопасности

	Используемые механизмы							
Услуги безопасности	Шифрование	Заполнение трафика	Управление маршрутизацией	Цифровая подпись	Контроль доступа	Обеспечение целостности	Аутентификация	Нотаризация (подтверждение)
Конфиденциальность (системы с установлением связи) Sec_{ete}		Да	Да					
Конфиденциальность (системы без установления связи)	Да	Да	Да					
Конфиденциальность (отдельные информационные поля) Sec_{fild}								
Конфиденциальность (трафик) Sec_{data}		Да						
Аутентификация отправителя данных A_{souce}	Да			Да		Да	Да	
Аутентификация равноправного логического объекта A_{obj}	Да			Да		Да	Да	
Целостность (с установлением связи) $Integr_{rec\_ete}$			Да			Да		
Целостность (без установления связи)	Да		Да			Да		
Целостность (отдельные информационные поля) $Integr_{fild}$	Да					Да		
Контроль доступа C_{acses}					Да			
Причастность (отправка и доставка)				Да				Да
Доступность			Да		Да		Да	

В таблице, где возможно использование услуг IEEE 802.10 (SDE), которые не специфицированы ISO, проставлен символ «?». Пустые ячейки указывают, что на данном уровне услугу не рекомендуется применять.

Услуги защиты информации предоставляются через интерфейс управления и/или h-службу вызова –совокупность функциональных возможностей h-уровня и нижележащих уровней, предоставляемых (h+1)-объектам на границе h и (h+1) -уровнями (в терминологии ЭМ ВОС). При каждом запросе h-службы (h +1)-объект может запросить желаемую цель защиты. В запросе указывается конкретная служба защиты, необходимые параметры службы и, при необходимости, - любая дополнительная релевантная информация (например, информация о грифе конфиденциальности и/или метка безопасности) в соответствии с целью защиты. Запрос h-услуги защиты, который формирует h+1 логический объект, определяет тип и параметры защиты и осуществляется через обращение к информационной базе административного управления защитой (ИБАУЗ). Параметры защиты могут устанавливаться по умолчанию. Планирование служб защиты должно достигаться одним или двумя следующими методами: а) непосредственным вызовом механизмов защиты в рамках h-уровня; б) и/или запросом служб защиты на (h–I)-уровне. В этом случае область применения защиты должна быть расширена на h-службу путем сочетания передоверяемых функциональных возможностей и/или специальных механизмов защиты на h-уровне. Таким образом, h-уровень определяет, способен ли он обеспечить требуемую защиту цели, если он неспособен, обеспечить это, то соединение блокируется.

Приведем планирование служб в рамках h-уровня (в противоположность передаче нижележащим (h-I)-службам) в процессе установления защищенного h-соединения:

а) Опережающий контроль доступа.

h-уровень может требовать опережающего контроля доступа, он может локально определять (от информационной базы управления защитой), может ли быть разрешено или запрещено защищенное h-соединение.

б) Аутентификация равноправных объектов.

Эта услуга, когда она предусмотрена h-уровнем, предназначена для выдачи подтверждения (h+I)-объекту, что источником данных является равноправный (h+I)-объект.

Если защита цели включает идентификацию равноправных объектов или если известно (из информационной базы управления безопасностью), что назначение h-объекта потребует идентификации равноправного объекта, то должен произойти идентификационный обмен. Для этого может использоваться двух- или трехкратное квитирование установления связи для обеспечения односторонней или взаимной идентификации. Идентификационный обмен может быть объединен либо с обычными процедурами установления h-соединения, либо осуществлен отдельно от установления h-соединения.

в) Контроль доступа.

Назначение h-объекта или промежуточных объектов может потребовать ограничений контроля доступа. Если специфическая информация затребована через механизм дистанционного контроля доступа, то h-объект, являющиеся инициатором, предоставляет эту информацию в рамках протокола h-уровня или через каналы управления.

г) Конфиденциальность.

Если была выбрана служба полной или избирательной конфиденциальности, то должно быть установлено защищенное h-соединение. Это может включать установление собственных рабочих ключей и обсуждение криптографических параметров соединения. Это может быть сделано путем предварительной компоновки в идентификационном обмене или путем отдельного протокола;

д) Целостность данных.

Эта служба, когда она предусмотрена h-уровнем, предназначена для выдачи подтверждения (h+I)-объекту, что источником данных является заявленный равноправный (h+I)-объект.

Если была выбрана целостность данных всех h-пользователей с восстановлением или без восстановления или целостность отдельных полей протокольного блока данных, то необходимо установить защищенное h-соединение. Оно может быть аналогично соединению с задействованием службы конфиденциальности и может предусматривать идентификацию. К защищенному h-соединению применимы те же соображения, что и для службы конфиденциальности;

е) Службы безотказности.

Если была выбрана безотказность с подтверждением происхождения, необходимо установить собственные криптографические параметры или установить защищенное соединение с объектом, осуществляющим нотаризацию.

Если была выбрана безотказность с подтверждением доставки, необходимо установить собственные параметры (которые отличаются от параметров, требуемых для безотказности с подтверждением происхождения) или установить защищенное соединение с объектом, осуществляющим нотаризацию.

В сеансе связи в процессе передачи данных по защищенному h-соединению должны быть задействованы конкретные службы защиты. При этом в рамках h-службы должно быть организовано:

а) идентификация равноправных объектов (в интервалах);

6) защита выбранных полей;

в) сигнализация об активных нападениях (например, службой «целостность соединения без восстановления» при возникновении манипуляций данными. Кроме того, может потребоваться запись ревизии следа защиты, обнаружение события и управление событием.

Механизмы защиты могут быть реализованы как в виде отдельных процедур, так и являться неотъемлемой частью протоколов установления

соединения. Механизмы защиты, предоставляющие реализующие услуги безопасности в рамках связных протоколов, будем моделировать системами массового обслуживания с протокольной услугой безопасности (СМОПб), а в рамках отдельных процедур – системами массового обслуживания с самостоятельной услугой безопасности (СМОСб). Последние, в том числе включают в себя формализацию процессов управления безопасностью и могут включать как фазы формирования и передачи сервисных примитивов трафика безопасности на дополнительном логическом уровне архитектуры сети, так и фазу их обработки в конечных и/или промежуточных системах с учетом QoS-норм передачи основных информационных потоков. В любом случае, реализация механизмов защиты осуществляется по принципам предоставления сервиса ВОС.

2.2.3. Общие механизмы обеспечения безопасности

В стандарте ГОСТ Р ИСО 7498-2-99 определены следующие общие механизмы обеспечения безопасности: доверительная функциональность, метки безопасности, "аудиторская" проверка. Другие общие механизмы обеспечения безопасности, как например, управление криптографическими ключами относятся к более высоким уровням интеграции систем и их менеджмента.

Доверительная функциональность

Доверительная функциональность является явным общим механизмом обеспечения безопасности. Доверительная функциональность включает множество рекомендаций и способов, которые должны быть реализованы для обеспечения гарантии (уверенности) правильной работы других механизмов безопасности. Для обеспечения надежной (доверительной) работы программного обеспечения, реализующего механизмы безопасности, необходимо соблюдать строгие спецификации и специальную технологию разработки, использование безопасных каналов распространения и многое другое. Аппаратные средства должна разрабатываться и проверяться на основе единой методики. На этом уровне также обеспечиваются все необходимые требования и рекомендация к электромагнитным излучениям и возможностям физического вмешательства.

Метки безопасности

Метки безопасности могут быть ассоциированы с отдельными пакетами или последовательностями явно или косвенно. Метки безопасности обычно используются для реализации политики доступа на основе правил, а также могут использоваться для управления маршрутизацией в сервисах обеспечения конфиденциальности. Возможно также применения меток для контроля целостности. Если метки безопасности применяются явно, то пакеты с такими метками должны быть защищены от нарушения целостности.

Контроль безопасности

Контроль безопасности включает множество механизмов: обнаружение попыток нарушения безопасности, анализ случаев успешного вмешательства и возникших потерь и др. Но при этом необходимо решение вопросов, какую информацию в системе следует накапливать и как ее потом анализировать. Проблемой при этом является определение того минимума информации, который бы позволил выявить (не пропустить) возможные события по вмешательству в работу компьютерной системы.

2.2.4. Анализ использования услуг безопасности на различных уровнях модели ВОС

В стандарте ГОСТ Р ИСО 7498-2-99 определена применимость различных услуг безопасности для различных уровней модели ВОС, которая может быть представлена в виде таблицы 2.2. Ячейки, обозначающие применимость даного типа услуги на определенном уровне модели ВОС, обозначены как "да". В ячейках, где возможно использование услуг IEEE 802.10 (SDE), которые не спицифицированы ISO, проставлен символ "?". Пустые ячейки указывают на то, что на данном уровне услугу не рекомендуется применять.

Таблица 2. 2 - Применимость сервисов безопасности на различных уровнях модели ВОС

	Уровни модели ВОС						
Услуга безопасности	1	2	3	4	5	6	7
Конфиденциальность (системы с установлением связи)	да	да	да	да			да
Конфиденциальность (системы без установления связи)		да	да	да			да
Конфиденциальность (отдельные информа- ционные поля)							да
Конфиденциальность (трафик)	да		да				да
Аутентификация		?	да	да			да
Целостность			да	да			да

(с установлением связи)							
Целостность (без установления связи)		?	да	да			да
Целостность (отдельные информа- ционные поля)							да
Контроль доступа		?	да	да			да
Причастность (отправка и доставка)							да

Физический уровень

Услуги безопасности, предлагаемые на Физическом уровне, обычно обеспечивают защиту каналов "точка-точка", например, между двумя конечными системами или между конечной и промежуточной системами. Действие этой услуги заканчивается в точке окончания канала перед устройством приема или коммутации пакетов.

Однако средства и устройства, обеспечивающие безопасность на этом уровне, обычно привязаны к конкретной технологии передачи сигналов и интегрированы с физическим интерфейсом, что приводит к необходимости использовать идентичные устройства на обоих концах физического и/или виртуального соединения. Применеие средств защиты Физического уровня ограничивается услугами Конфиденциальности для коммуникаций с установлением связи и для защиты от контроля трафика. Другим ограничением использования средств защиты на Физическом уровне является сложность управления ими.

Бит- ориентированный интерфейс Физического уровня не позволяет реализовать услуги Целостности и Аутентификации из-за невозможности выполнять преобразование данных. Однако использование подходящей техники шифрования на этом уровне может создать хорошую базу для использования услуг на более высоких уровнях.

Канальный уровень

Услуги безопасности Канального уровня реализуются для соединений "точка- точка" аналогично Физического уровня. Действие этой услуги заканчивается в точке приема (конечная система) или коммутации пакетов (включая транслирующие и инкапсулирующие мосты) в пределах использования единого интерфейса управления доступом к среде (УДС, МАС-интерфейса). Преимуществом применения услуг безопасности на этом

уровне является их независимость от протоколов более высокого уровня. Однако здесь также существует сильная зависимость практической реализации услуги от используемой технологии Физического уровня.

Согласно рекомендациям стандарта ГОСТ Р ИСО 7498-2-99 услуги, предлагаемые на этом уровне включают Конфиденциальность для систем с установлением и без установления связи. Возможность использования этого уровня для обеспечения услуг Целостности ограничивается недостаточным размером контрольных полей LLC- пакетов.

Сетевой уровень

Безопасность на Сетевом уровне обеспечивается между конечными системами, независимо от промежуточных межсетевых коммутаторов и мостов уровня Данных. Если услуги безопасности основываются полностью на протоколах Сетевого уровня, это обеспечивает безопасность коммуникаций между конечными системами вдоль разнородных сетей, формирующих Интерсеть (Internet). Стандарт ГОСТ Р ИСО 7498-2-99 рекомендует применение нескольких услуг безопасности на Сетевом уровне: Конфиденциальность (для систем с установлением и без установления связь, для защиты от контроля трафика), Контроль доступа, Целостность в системах с установлением связи и без, а также Аутентификации источника данных и объекта коммуникации.

Согласно рекомендациям ГОСТ Р ИСО 7498-2-99 услуги безопасности должны быть совместимы с соответствующими коммуникационными услугами на каждом уровне и, по возможности, их использовать, что часто приводит к зависимости реализуемых услуг безопасности от протоколов сетевого уровня или делает невозможным их применение. Такая ситуация, в частности, наблюдается в сетях, которые имеют свой собственный протокол нумерации последовательностей с установлением связи, но не имеют средств обеспечения целостности отдельных пакетов, что делает невозможным применение стандартных услуг безопасности. В этом случае возможно применение соответствующих услуг на более высоких уровнях, но приводит к зависимости услуг безопасности от соответствующей технологии Сетевого уровня.

Услуги безопасности, полностью использующие протоколы Сетевого уровня, т.е. реализуемые "поверх" Сетевого уровня, могут обеспечивать защищенность коммуникаций в многопротокольных интерсетях. При этом услуги безопасности могут быть реализованы в межсетевых (или "промежуточных" - intermediate) системах или устройствах. Это дает ряд преимуществ, связанных с тем, что межсетевые устройства часто служат шлюзами или портами между различными локальными или локальными и глобальными сетями. Обеспечение услуг безопасности и защищенности в таких пограничных устройствах эффективно с точки зрения минимальной модернизации существующих систем. Дополнительные средства

безопасности могут быть обеспечены между межсетевыми устройствами и конечными системами, используя те же протоколы и услуги.

Независимая реализация услуг безопасности на Сетевом уровне позволяет применять эти услуги только в отношении таких объектов, как сети, что является достаточно "грубым" подходом. Для отдельных групп сетевых протоколов существуют возможности обеспечить избирательность таких услуг, основываясь на адресации конкретных конечных систем или при использовании дополнительных средств для адресации протоколов более высокого уровня в протоколах Сетевого уровня, как это сделано в протоколах TCP/IP с адресацией вышестоящих протоколов и портов в пакетах Сетевого и Транспортного уровня. Однако это нарушает принцип уровневости и, в общем случае, неприменимо.

Дополнительная возможность для обеспечения избирательности услуг безопасности на Сетевом уровне может быть реализована через параметр "качества услуги" безопасности, определяемый конечной системой и обрабатываемый промежуточными системами. В частности, разрабатываемый стандарт безопасного протокола Сетевого уровня (NLSP - Network Layer Security Protocol) предполагает такую возможность.

Включение услуг безопасности Сетевого уровня в состав функций конечной системы, как правило, требует модификации ядра операционной системы, так как большинство сетевых операционных систем включают функции сетевого уровня в ядро в целях достижения большей производительности и безопасности системы. Отсюда следует, что включение услуг безопасности Сетевого уровня является задачей поставщиков программных и аппаратных средств конечных и промежуточных систем.

Транспортный уровень

На Транспортном уровне стандарт ГОСТ Р ИСО 7498-2-99 определяет набор услуг безопасности, очень близкий по составу с Сетевым уровнем: Конфиденциальность (для систем с установлением и без установления связи), Контроль доступа, Целостность в системах с установлением связи и без, а также Аутентификации источника данных и обьекта коммуникации. Отличием является то, что услуги безопасности Транспортного уровня обеспечиваются только в конечных системах, в отличие от возможности релизации услуг на базе Сетевого уровня в промежуточных системах.

Услуги безопасности Транспортного уровня с установлением связи, в общем случае, обеспечивают более высокую защищенность коммуникаций по сравнению с реализацией таких же услуг на более высоких уровнях с использованием протоколов и услуг более низкого уровня. Но при правильном использовании коммуникационных возможностей Транспортного уровня такие отличия могут быть несущественными.

Так же как и для Сетевого уровня, многие механизмы безопасности Транспортного уровня интегрированы в состав сетевых операционных систем и определяется их разработчиками.

Сеансовый уровень и уровень Представления данных

ГОСТ Р ИСО 7498-2-99 не рекомендует применение услуг безопасности на Сеансовом уровне и уровне Представления данных. Это вызвано тем, что эти уровни не имеют хорошо определенных коммуникационных услуг и функций. Кажущаяся уместность применения многих услуг на основе шифрования на уровне Представления данных нецелесообразна из-за того, что функции этого уровня обычно интегрированы в состав Прикладного уровня.

Прикладной уровень

Стандарт ГОСТ Р ИСО 7498-2-99 разрешает применение всех услуг безопасности на Прикладном уровне, а применение услуги Причастности рекомендуется только на этом уровне. Однако использование услуг безопасности только на Прикладном уровне не позволяет полностью защитить системы коммуникаций от всех возможных атак, поэтому рекомендуется обеспечивать поддержку конкретных услуг также на более низких уровнях совместно с Прикладным.

Наиболее привлекательной чертой применения услуг безопасности на Прикладном уровне является их независимость от операционной системы и возможность реализовать эти услуги в составе приложений, но при этом используемые механизмы становятся специфическими для конкретного приложения.

2.2.5. Определение приоритетов применения базовых услуг безопасности в ИС

Политика информационной безопасности ИС, в зависимости от е назначения, может строится в соответствии с различными приоритетами реализации базовых услуг безопасности в порядке убывания их важности. Один из примеров такой реализации

- *доступность* информации (обеспечение устойчивого функционирования системы);
- *целостность* хранимой, обрабатываемой и передаваемой по каналам связи информации;
- *конфиденциальность* хранимой, обрабатываемой и передаваемой по каналам связи информации.

Нарушения доступности информационных, программных и аппаратных ресурсов может привести к дезорганизации процесса обработки информации (несанкционированный останов СУБД, ОС, уничтожение данных и так далее).

Нарушение целостности данных, а также программных компонентов ИС, находящихся как на сервере, так и на рабочих станциях может привести

к некорректному функционированию программного обеспечения и преодолению системы защиты. Нарушитель, поразив целостность компонент ИС, может заблокировать ее нормальное функционирование и тем самым осуществить атаку на доступность системы.

Нарушение конфиденциальности может привести к разглашению или утечке информации из ИС и нанесению материального и морального ущерба юридическим или физическим лицам, обслуживаемым ИС, а так же к несанкционированному предоставлению привилегий пользователям СУБД и ОС, что может повлечь доступ и искажение информации в ИС и служебной информации файлов аудита СУБД и ОС.

Нарушитель, поразив конфиденциальность компонент автоматизированной системы (например, перехватив административные пароли) может исказить какой либо конфигурационный файл и тем самым осуществить атаку на целостность и доступность системы.

В данном примере на первом месте выступает базовая услуга безопасности «Доступность», что характерно для ИС общего пользования, например, ИС заказа авиа- или железнодорожных билетов. Для специальных ИС специального и военного назначения на первое место всегда выступает базовая услуга безопасности «Конфиденциальность».

2.3. Проведение анализа рисков

2.3.1. Анализ рисков в ИС

Анализ рисков — это то, с чего должно начинаться построение политики ИБ ИС. Он включает в себя мероприятия по обследованию безопасности ИС, целью которых является определение того, какие активы ИС и от каких угроз надо защищать, а также в какой степени те или иные активы нуждаются в защите.

В процессе анализа рисков проводятся следующие работы:

- идентификация всех активов в рамках выбранной области деятельности;
- определение ценности идентифицированных активов;
- идентификация угроз и уязвимостей для идентифицированных активов;
- оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;
- выбор критериев принятия рисков;
- подготовка плана обработки рисков.

Необходимо идентифицировать только те активы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности. Важность (или стоимость) актива определяется величиной ущерба, наносимого в случае нарушения его конфиденциальности, целостности или доступности. В ходе оценки стоимости активов

определяется величина возможного ущерба для каждой его категории при успешном осуществлении угрозы.

Оценка уязвимостей активов ИС, обусловленных слабостями их защиты, предполагает определение вероятности успешного осуществления угроз безопасности. Под уровнем угрозы понимается вероятность ее осуществления. Оценка угроз включает в себя

- определение уязвимых мест системы;
- анализ вероятности угроз, направленных на использование этих уязвимых мест;
- оценка последствий успешной реализации каждой угрозы;
- оценка стоимости возможных мер противодействия;
- выбор оправданных механизмов защиты (возможно, с использованием стоимостного анализа).

Таким образом, величина риска определяется на основе стоимости актива, уровня угрозы и величины уязвимости. С увеличением стоимости актива, уровня угрозы и величины уязвимости возрастает и величина риска. На основе оценки величины рисков определяются требования безопасности.

Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину, т. е. дать им количественную оценку. Оценка рисков включает в себя:

- идентификация ключевых (критичных) активов ИС;
- определение важности тех или иных активов;
- идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз;
- вычисление рисков, связанных с осуществлением угроз безопасности.

Определение набора адекватных контрмер осуществляется в ходе построения подсистемы ИБ ИС и управления рисками. Задача управления рисками включает выбор и обоснование выбора контрмер, позволяющих снизить величину рисков до приемлемого уровня. Управление рисками включает в себя оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше вероятность причинения ущерба. Контрмеры могут способствовать уменьшению величины рисков различными способами:

- уменьшая вероятность осуществления угроз безопасности;
- ликвидируя уязвимости или уменьшая их величину;
- уменьшая величину возможного ущерба;
- выявляя атаки и другие нарушения безопасности;
- способствуя восстановлению ресурсов ИС, которым был нанесен ущерб.

Таким образом, работы по анализу и управлению рисками, можно условно разделить на три последовательных этапа. Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты системы применения средств базового уровня, реализующих функции безопасности в порядке их

приоритета, или необходимо проведение более детального анализа защищенности?». На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер.

В процессе оценки защищенности информационной системы определяются угрозы, действующие на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз. Угрозы и уязвимости рассматриваются только во взаимосвязи друг с другом (т.к. ***Инцидент*** - событие, указывающее на действительную, мнимую или вероятную реализацию угрозы, возникает в случае появления комплиментарной пары «угроза-уязвимость»). Уязвимость, через которую невозможно реализовать ни одну из угроз, не имеет смысла. Аналогично, угроза, которую невозможно реализовать ввиду отсутствия уязвимости, также неактуальна.

2.3.2. Перечни критичных ресурсов в ИС. Категорирование ресурсов

В ИС предприятия хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации. Прежде всего, следует определить**,** что является ***ценным активом*** компании с точки зрения информационной безопасности. Стандарт ISO 17799, подробно описывающий процедуры системы управления ИБ, выделяет следующие виды активов:

• информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.);

• программное обеспечение,

• материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.);

• сервисы (поддерживающая инфраструктура);

• сотрудники компании, их квалификация и опыт,

• нематериальные ресурсы (репутация и имидж компании).

Следует определить, нарушение информационной безопасности, каких активов может нанести ущерб компании. В этом случае актив будет считаться ценным, и его необходимо будет учитывать при анализе информационных рисков.

Инвентаризация заключается в составлении перечня ценных активов компании. Как правило, данный процесс выполняют владельцы активов.

Различаются следующие категории информационных ресурсов, подлежащих защите в предприятия:

- Информация, составляющая коммерческую тайну;
- Информация, составляющая служебную тайну;
- Персональные данные сотрудников;

- Конфиденциальная информация (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне;
- Данные, критичные для функционирования ИС и работы бизнес подразделений.

Первые четыре категории информации представляют собой сведения ограниченного распространения, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности информации путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

К последней категории «критичных» данных, относятся информационные ресурсы предприятия, нарушение целостности или доступности которых может привести к сбоям функционирования ИС либо бизнес подразделений.

В процессе категорирования активов необходимо оценить их критичность для бизнес-процессов компании или, другими словами, определить, какой ущерб понесет компания в случае нарушения информационной безопасности активов.

Данный процесс вызывает наибольшую сложность, так как *ценность активов определяется на основе экспертных оценок их владельцев***.** В процессе данного этапа часто проводятся обсуждения между консультантами по разработке системы управления и владельцами активов. Это помогает последним понять, каким образом следует определять ценность активов с точки зрения информационной безопасности (как правило, процесс определения критичности активов является для владельца новым и нетривиальным). Кроме этого, для владельцев активов разрабатываются различные методики оценки. В частности, такие методики могут содержать конкретные критерии (актуальные для данной компании), которые следует учитывать при оценке критичности.

Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности (следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов).

Оценку критичности активов можно выполнять в денежных единицах и в уровнях. Однако, учитывая тот факт, что для анализа информационных рисков необходимы значения в денежных единицах, в случае оценки критичности активов в уровнях, следует определить оценку каждого уровня в деньгах. Например, для базовой оценки рисков достаточно 3-уровневой шкалы оценки критичности - низкий, средний и высокий уровни.

При выборе шкалы важно учитывать следующее:

• чем меньше количество уровней, тем ниже точность оценки;

• чем больше количество уровней, тем выше сложность оценки (то есть сложно определить разницу между, скажем, 7-м и 8-м уровнем 10-ти уровне вой шкалы).

Следовательно, в этом вопросе нужно найти «золотую середину», чтобы и точность не очень пострадала, и сложность не превышала допустимых пределов.

Кроме этого, следует иметь в виду, что для расчета информационных рисков достаточно примерных значений критичности активов: не обязательно оценивать их с точностью до денежной единицы. Однако денежное выражение критичности все равно необходимо.

Рассмотрим подробнее принципы оценки критичности каждого указанного актива.

- Информационные активы (или виды информации) оцениваются с точки зрения нанесения компании ущерба от их раскрытия, модификации или недоступности в течение определенного времени.
- Программное обеспечение, материальные ресурсы и сервисы оцениваются, как правило, с точки зрения их доступности или работоспособности. То есть требуется определить, какой ущерб понесет компания при нарушении функционирования данных активов. Например, нарушение системы кондиционирования в течение трех суток приведет к отказу серверов компании, к ним будет нарушен доступ, и вследствие этого компания понесет убытки.
- Сотрудники компании с точки зрения конфиденциальности и целостности оцениваются, учитывая их доступ к информационным ресурсам с правами на чтение и на модификацию. Доступность сотрудников оценивается с точки зрения их отсутствия на рабочем месте. Другими словами, оценивается, какой ущерб понесет компания при отсутствии сотрудника в течение определенного периода времени. Здесь важно учесть опыт сотрудника, его квалификацию, выполнение им каких-либо специфических операций.
- Репутация компании оценивается в связи с информационными ресурсами: какой ущерб репутации компании будет нанесен в случае нарушения безопасности информации компании.

Заметим, что процесс категорирования активов должен подчиняться четким документированным процедурам компании. Аудиторам сертификационного органа будет недостаточно формального документа, отражающего результаты категорирования. От владельцев активов требуется, чтобы они могли объяснить, какие методики они использовали при оценке, на основании каких данных были получены результаты оценки.

2.3.3. Оценка защищенности информационной системы

Очевидно, что для анализа информационных рисков необходимо оценить не только критичность активов, но и уровень их защищенности.

В процессе оценки защищенности информационной системы определяются угрозы, действующие на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые

могут привести к реализации угроз. Угрозы и уязвимости рассматриваются только во взаимосвязи друг с другом (т. к. Инцидент - событие, указывающее на действительную, мнимую или вероятную реализацию угрозы, возникает в случае появления комплиментарной пары «угроза-уязвимость»). Уязвимость, через которую невозможно реализовать ни одну из угроз, не имеет смысла. Аналогично, угроза, которую невозможно реализовать ввиду отсутствия уязвимости, также неактуальна.

Не вызывает сомнения, что различные угрозы и уязвимости имеют разное значение (разный вес) для информационной системы. Например, злоумышленник скорее решит воспользоваться открытой дверью, чем открытым окном, если офис организации расположен на семнадцатом этаже 34-этажного здания (однако совсем исключать вторую возможность не стоит). Следовательно, необходимо определить, какие угрозы и уязвимости наиболее актуальны, а какие менее значимы, или, другими словами, определить вероятность реализации угрозы через уязвимость. Вероятность реализации уязвимостей (как и любая другая вероятность) определяется в пределах от 0 до 1 (или от 0 до 100 %).

Угрозы, уязвимости, а также их вероятности определяются в результате проведения технологического аудита защищенности информационной системы организации. Такой аудит может быть выполнен как специалистами организации (так называемый, внутренний аудит), так и сторонними консультантами (внешний аудит).

2.3.4. Оценка информационных рисков (оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов)

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей.

С количественной точки зрения классическая формула оценки уровня риска есть произведение вероятности реализации определенной угрозы (использующей некоторые уязвимые места), на величину возможного ущерба: R=P(V) *D, где R - информационный риск; D - критичность актива (ущерб); P(V) - вероятность реализации уязвимости.

Результаты оценки рисков, как правило, представляются в «Отчете об оценке информационных рисков компании».

2.3.5. Обработка информационных рисков (выбор критериев принятия рисков, подготовка плана обработки рисков)

Обработка информационных рисков - это этап, в процессе которого определяется, какие действия по отношению к рискам требуется выполнить в компании.

Основными способами обработки рисков являются:

- принятие рисков;

• уклонение от рисков;
• передача рисков;
• снижение рисков.

Принятие рисков осуществляется в том случае, если уровень рисков признается приемлемым, то есть компания не считает целесообразным применять какие-либо меры по отношению к этим рискам и готова понести ущерб.

Уклонение от рисков это полное устранение источника риска.

Передача рисков — перенесение ответственности за риск на третьи лица (например, поставщика оборудования или страховую компанию) без устранения источника риска.

Снижение рисков - это выбор и внедрение мер по снижению вероятности нанесения ущерба.

В процессе обработки рисков сначала требуется определить, какие из них требуют дальнейшей обработки, а какие можно принять. Как правило, это решается с помощью оценки приемлемого уровня риска. Риски, равные или ниже приемлемого, можно принять. Очевидно, что для рисков, превышающих приемлемый уровень, требуется выбрать дальнейшие меры по обработке. Приемлемый уровень риска определяется руководством компании или специальной группой, в которую входят руководители и главные финансисты компании. Например, если руководство компании декларирует, что низкий уровень риска считается приемлемым, то дальнейшие действия по обработке рисков определяются только для средних и высоких уровней риска. Причем, средний и высокий уровни риска требуется снизить до низкого (то есть до приемлемого) уровня.

В случае, когда в компании наблюдается большой разброс значений риска (как правило, это может возникнуть, если критичность активов была определена в денежных единицах, а не уровнях), информационные риски можно разбить на категории и определять приемлемый уровень для каждой из них отдельно. Это вызвано тем, что снижать различные значения рисков до одного заданного значения не всегда целесообразно (часто для снижения высоких рисков до заданного уровня необходимы неоправданно большие затраты).

По результатам данного этапа требуется составить «*Отчет об обработке информационных рисков компании*», который подробно описывает способы обработки рисков. Кроме этого, составляется «*План снижения рисков*», где четко описываются конкретные меры по снижению рисков, сотрудники, ответственные за выполнение каждого положения плана, сроки выполнения плана. Данный документ содержит перечень первоочередных мероприятий по снижению уровней рисков, а также цели и средства управления, направленные на снижение рисков, с указанием:

- лиц, ответственных за реализацию данных мероприятий и средств;
- сроков реализации мероприятий и приоритетов их выполнения;
- ресурсов для реализации таких мероприятий;

- уровней остаточных рисков после внедрения мероприятий и средств управления.

2.4. Модели нарушителя в ИС

2.4.1. Модель нарушителя в «закрытом» контуре

В «закрытом» контуре модель нарушителя и угроз строится с учетом обеспечения следующей архитектуры приоритетов базовых услуг безопасности 1) конфиденциальность, 2) целостность и 3) доступность активов «закрытого» контура.

Под нарушителем понимается человек или группа лиц, имеющая своей целью нанесение целью нанесения ущерба пользователям ИС в целом путем преодоления (нарушения) целевых функций, реализуемых подсистемой защиты информации «закрытого» контура ИС и нанесением удара на конфиденциальность, доступность и целостность «закрытого» контура.

Нарушителем может быть как физическое лицо, так и некоторый процесс, выполняющийся на вычислительных средствах «закрытого» контура. Все физические лица, имеющие доступ к ресурсам ИС, могут быть отнесены к следующим категориям:

- категория I - лица, не имеющие права доступа в контролируемую зону, в которой располагаются ресурсы ИС;
- категория II - лица, имеющие право постоянного или разового доступа в контролируемую зону, в которой располагаются ресурсы ИС.

Нарушители из числа лиц категории I являются внешними нарушителями, а из числа лиц категории II - внутренними нарушителями.

Предполагается, что все лица рассмотренных категорий и классов относятся к потенциальным нарушителям.

При разработке Модели нарушителя предполагается, что

- внешний нарушитель может проводить атаку только из-за пределов контролируемой зоны;
- физическое проникновение внешнего нарушителя на объект защиты с целью внедрения в «закрытый» контур ИС программных средств скрытого информационного воздействия (ПССИВ, например, компьютерные вирусы, программные закладки, эксплоиты и т. д.) исключено;
- осуществление атак внешним нарушителем посредством перехвата секретной информации и последующего ее анализа в каналах связи

межсетевого обмена «закрытого» контура и системами Ведомственного сегмента, защищенных СКЗИ, исключено и малоэффективно с учетом степени защищенности используемых каналов связи, стоимости и времени на проведение криптоанализа и времени потери ценности перехваченной информации;

- организационными мерами исключается возможность реализации атак на закрытый контур со стороны внешнего нарушителя (в том числе, реализации каналов выноса информации) за счет использования неучтенных носителей внутренним нарушителем - пользователем «закрытого» контура ИС;
- организационными мерами (контроль за соблюдением правил работы с носителями, установленными ведомственными инструкциями) исключается попадание к внешнему нарушителю секретной информации из закрытого «закрытого» контура с использованием учтенных носителей пользователей;
- для реализации атак на «закрытый» контур внешний нарушитель не использует недекларированные возможности программных компонент, совместно с которыми предполагается штатное функционирование средств защиты информации;
- осуществление внешних атак на «закрытый» контур через «открытый» контур исключено ввиду организации двойного экранирования: межсетевое взаимодействие «открытого» контура с внешними системами должно осуществляться только через «демилитаризационные зоны», а с «закрытым» контуром только через однонаправленный шлюз. Межсетевое взаимодействие «закрытого» контура с внешними системами через «открытый» контур запрещено.

В модели нарушителя «закрытого» контура ИС предположительно должны быть учтены следующие группы потенциальных нарушителей:

- внешний нарушитель (далее - нарушитель группы Н1), не являющийся пользователями «закрытого» контура - субъект, имеющий доступ на контролируемую территорию ИС, но не имеющие доступа к работе со штатными средствами «закрытого» контура. К этой группе нарушителей относится администратор ЛВС «открытого» контура. Нарушитель данной группы осуществляет атаки, используя возможности по доступу к информации, передаваемой по соответствующим протоколам информационного обмена, с целью внедрения в «закрытый» «закрытый» контур ИС. Администратор ЛВС «открытого» контура имеет возможность производить разграничение доступа к секретной информации, используя штатные средства защиты, не имея фактического доступа к преобразованной информации на сервере, а также производить ее архивирование. Администратор ЛВС как лицо, обладающее максимальными полномочиями по администрированию сетевой операционной системы «открытого» контура, имеет

максимальные возможности для внесения «программ-закладок» через однонаправленный шлюз в «закрытый» контур;

- внешний нарушитель (далее - нарушитель группы Н2), осуществляющий атаки с удаленных рабочих мест корпоративной сети. Нарушитель данной группы осуществляет атаки, используя возможности по доступу к информации, передаваемой по соответствующим протоколам информационного обмена, с целью внедрения в «закрытый» «закрытый» контур ИС;
- внутренний нарушитель не являющийся пользователем «закрытого» контура ИС и не имеющий доступа к информации и работе со штатными средствами (далее - нарушитель группы Н3). К данной группе относятся:

а) сотрудники организации, имеющие санкционированный доступ в помещения, в которых размещается оборудование компонентов ИС;

б) эксплуатационно-технический персонал «закрытого» контура (работники инженерно-технических служб и т. д.);

в) уполномоченный персонал разработчиков ИС СН, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС СН под контролем пользователей.

- внутренний нарушитель не являющийся пользователем «закрытого» контура ИС и не имеющий доступа к работе со штатными средствами ИС, но пытающийся нарушить конфиденциальность обрабатываемой в закрытом «закрытом» контуре ИС информации (далее именуемый - нарушитель Н4).
- внутренний нарушитель (далее - нарушитель группы Н5), являющийся легальным пользователем «закрытого» контура, имеющий доступ к работе со штатными средствами «закрытого» контура и возможность обработки информации в системе, но пытающиеся получить доступ к объектам защиты «закрытого» контура в нарушение предоставленных им полномочий. К данной группе нарушителей относятся операторы «закрытого» контура;
- внутренний нарушитель (далее - нарушитель группы Н6), являющийся привилегированным легальным пользователем «закрытого» контура, имеющий доступ к работе со штатными средствами «закрытого» контура, но пытающиеся получить доступ к объектам защиты «закрытого» контура в нарушение предоставленных им полномочий. К данной группе нарушителей относятся

а) администратор СУБД (Н6а) отвечает за управление и конфигурирование СУБД, обеспечение непрерывного сервиса СУБД. Выполняет процедуры подготовки резервного копирования. Является экспертом в области администрирования применяемой СУБД. Владеет информацией о физической структуре СУБД, ее компонентах, концепциях и стратегиях применения. Имеет все возможности по настройке параметров СУБД, включая

возможности добавления и удаления пользователей, присвоения привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД. Может произвести действия, нарушающие безопасность СУБД и обрабатываемых данных «закрытого» контура.

б) администратор БД (Н6б) занимается разграничением прав доступа к объектам БД, управляет созданием, модификацией и удалением объектов. Администратор БД владеет информацией о логической структуре данных, имеет представление о хранимой информации, привилегиях доступа пользователей к данным. Может произвести действия, нарушающие безопасность обрабатываемых данных АСЗИ.

в) администратор ОС (Н6в) занимается управлением и конфигурированием ОС. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы СУБД и клиентов системы. Администратор ОС является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС. Владеет информацией об особенностях конфигурации, параметров настройки и организации функционирования БД в данной ОС. Имеет все возможности по настройке параметров ОС, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, удаление журнала аудита ОС. Может произвести действия, нарушающие безопасность ОС, СУБД и обрабатываемых данных в «закрытом» контуре.

г) администратор аппаратной платформы (АП) (Н6г) занимается управлением и конфигурированием аппаратной платформы. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы ОС и поддерживаемых ею приложений. Администратор АП является экспертом в области используемой аппаратной платформы, владеет информацией об используемых физических устройствах, аппаратной конфигурации системы. Не имея непосредственного доступа к информации БД, обеспечивает функционирование СУБД и прикладного ПО.

д) администратор ПСЗИ «закрытого» контура (Н6д) имеет полномочия по предоставлению прав пользователям и управлению регистрационными журналами ПСЗИ. Обеспечивает настройку систем защиты от НСД, систем криптографической защиты информации. Предоставляет полномочия и списки доступа в системах защиты от НСД.

При разработке мероприятий по защите информации в «закрытом» контуре ИС СН необходимо также предусмотреть возможные несанкционированные действия разработчиков ИС СН на этапах ее

разработки, внедрения и сопровождения. Возможными направлениями несанкционированных действий внутреннего нарушителя являются:

- доступ к защищаемой информации с целью нарушения ее конфиденциальности (хищение, ознакомление с информацией);
- доступ к информации с целью нарушения ее целостности (модификация информации);
- доступ к программно-техническим средствам с целью постоянного или временного нарушения доступности информации;
- использование ЭУНПИ в режимных помещениях и других ТС.

Внутренний нарушитель также может проводить атаку из-за пределов контролируемой зоны. Предполагается, что доступ к защищаемой информации внутренний нарушитель может получить путем:

- преодоления (обхода) системы разграничения доступа;
- использования специальных программных средств или не декларированных возможностей легально используемого ПО;
- перехвата акустической информации;
- визуального съема информации, выводимой на средства отображения;
- перехвата из-за пределов контролируемой зоны и анализа сигналов (в том числе, побочных), сопровождающих функционирование программно-технических средств ЛВС «закрытого» контура, а также передаваемых в сетях связи.

Кроме того, внутренний нарушитель может также предпринимать действия, приводящие к недоступности защищаемой информации для легального пользователя или к ее искажению (в том числе навязыванию ложной информации).

Внутренний нарушитель может предпринимать указанные действия на всех этапах жизненного цикла ИС и ее компонентов (установка и наладка технических средств, разработка и настройка ПО, эксплуатация, модернизация, вывод из эксплуатации или ремонт программно-технических средств), а также на всех технологических этапах обработки информации и во всех режимах функционирования программно-технических средств «закрытого» контура ИС.

При рассмотрении возможных действий внутреннего нарушителя считаются выполненными следующие ограничения и предположения:

- все зарегистрированные пользователи «закрытого» контура имеют не ниже 3 формы допуска;
- работа по подбору кадров и специальные мероприятия исключают возможность сговора между внутренним и внешним нарушителями, создания коалиций нарушителей, то есть объединения (сговора) и целенаправленных действий двух и более пользователей по преодолению ПСЗИ «закрытого» контура;
- организационно-техническими и режимными мерами исключен несанкционированный доступ в выделенные помещения, к программно-техническим средствам «закрытого» контура, структурированной

кабельной системе, к системам электропитания и заземления, а также пронос фото-, видео устройств, сотовых телефонов и иных не разрешенных к применению ТС и ЭУНПИ;

- внутренний нарушитель скрывает свои несанкционированные действия от других сотрудников;
- нарушения могут быть следствием непреднамеренных ошибок пользователей, администраторов, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности внутренний нарушитель может использовать любое имеющееся в его распоряжении средство съема и перехвата информации, воздействия на информацию и технические средства «закрытого» контура только из-за пределов контролируемой зоны;
- в «закрытом» контуре предпринимаются меры по обеспечению контролируемой зоны, исключающие бесконтрольное пребывание и действия лиц и/или транспортных средств (пропускной режим, средства инженерно-технической защиты), пронос фото-, видео устройств, сотовых телефонов и иных не разрешенных к применению ТС и ЭУНПИ.
- захват объекта противником считается исключенным.

Предполагается, что внешний нарушитель:

- обладает общими знаниями по порядку эксплуатации ПЗИ «закрытого» контура (нарушители Н2);
- знает характерные особенности функционирования (технологию использования и структуру) «закрытого» контура ИС (нарушители Н2);

Внешний нарушитель может осуществлять атаки:

- на технические средства «закрытого» контура ИС;
- на каналы связи, выходящие за пределы контролируемой зоны объектов ИС, используемые для передачи информации ограниченного доступа, с целью перехвата данной информации и последующего ее анализа, уничтожения, модификации, блокирования доступа к ней, а также реализации попыток преодоления ПСЗИ «закрытого» контура, навязывания ложной информации и нарушения работоспособности «закрытого» контура ИС в целом и ее отдельных компонент;
- посредством перехвата побочных электромагнитных излучений и наводок вне контролируемой зоны объектов, на которых располагаются технические средства «закрытого» контура ИС, и их последующего анализа;
- посредством перехвата сигналов, циркулирующих в сети питания и шине заземления (при возможности контактного подключения к ним за пределами контролируемой зоны);
- на помещения «закрытого» контура ИС, в которых циркулирует секретная акустическая информация.

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

Предполагается, что внутренний нарушитель, являющийся пользователем «закрытого» контура ИС (нарушители Н4, Н5 и Н6):

- является специалистом средней квалификации, не обладающим знаниями по разработке и тестированию (отладке) программного обеспечения (Н4, Н5);
- является специалистом высшей квалификации, обладающим знаниями по разработке и тестированию (отладке) программного обеспечения (Н6);
- является экспертом в области администрирования применяемой СУБД. Обладает возможностями по управлению и конфигурированию СУБД. Владеет информацией о физической структуре СУБД, ее компонентах, концепциях и стратегиях применения. Имеет все возможности по настройке параметров СУБД, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД (Н6а).
- обладает возможностями по разграничению прав доступа к объектам БД, управляет созданием, модификацией и удалением объектов, владеет информацией о логической структуре данных, имеет представление о хранимой информации, привилегиях доступа пользователей к данным (Н6б).
- является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС, владеет информацией об особенностях конфигурации, параметров настройки и организации функционирования БД в данной ОС. Обладает возможностями по управлению и конфигурированию ОС. Имеет все возможности по настройке параметров ОС, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, удаление журнала аудита ОС (Н6в).
- является экспертом в области используемой аппаратной платформы, владеет информацией об используемых физических устройствах, аппаратной конфигурации системы. Обладает возможностями по управлению и конфигурированию аппаратной платформы ЛВС «закрытого» контура, а также максимальными полномочиями по администрированию сетевой операционной системы. Имеет максимальные возможности для внедрения «программ-закладок» (скрытых программных воздействий) в программное обеспечение ТС «закрытого» контура не имея непосредственного доступа к информации БД, обеспечивает функционирование СУБД и прикладного ПО «закрытого» контура.

- имеет возможность по предоставлению и изменению полномочий и списков доступа в системах защиты от НСД и управлению регистрационными журналами СЗИ «закрытого» контура. Обладает максимальными правами по настройке систем защиты от НСД (Н6д).
- имеет данные об организации работы, структуре и используемых технических, программных и программно-технических средствах «закрытого» контура ИС (Н5, Н6);
- обладает знаниями по порядку эксплуатации ПСЗИ (Н5, Н6);
- знает характерные особенности функционирования (технологию использования и структуру) «закрытого» контура ИС (только для нарушителя Н5, Н6);
- имеет сведения об информационных ресурсах «закрытого» контура ИС: порядок и правила создания, хранения и передачи информации, структуре и свойствах информационных потоков (только для нарушителя Н5, Н6);
- располагает данными о реализованных в «закрытом» контуре ИС средствах защиты информации, включая описания используемых в шифровальных (криптографических) средствах криптографических алгоритмов и протоколов, описанием используемых криптографических алгоритмов (только для нарушителя Н5, Н6);
- может иметь данные об уязвимостях «закрытого» контура ИС, использующих недокументированные (не декларированные) возможности технических, программных и программно-технических средств «закрытого» контура ИС (только для нарушителя Н5, Н6);
- обладает возможностями по несанкционированным действиям с использованием штатных средств «закрытого» контура ИС (Н4, Н5, Н6);
- имеет физический доступ к техническим средствам и линиям связи в пределах выделенных ему полномочий, осуществляет легальный доступ к программно-аппаратным средствам и информации со своего рабочего места в соответствии с установленными для него полномочиями, но может пытаться получить доступ к ресурсам «закрытого» контура ИС, выходящий за пределы его полномочий (Н4, Н5, Н6);
- имеет сведения о возможных для «закрытого» контура ИС каналах атак (только для нарушителя Н5, Н6);
- знает информацию о способах (методах) атак на «закрытый» контур ИС (только для нарушителя Н5, Н6).

Предполагается, что внутренний нарушитель, не являющийся пользователем «закрытого» контура ИС (Н3), может получить физический доступ к техническим средствам, линиям связи, системам электропитания и заземления «закрытого» контура ИС при выполнении им обязанностей по регламентному обслуживанию данных средств. Возможности внутреннего нарушителя Н3 существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основными

являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- исключение несанкционированного допуска физических лиц в контролируемую зону и к программно-техническим средствам;
- контроль порядка проведения работ.

Внутренний нарушитель этого типа может осуществлять:

- непреднамеренные (ошибочные) действия при выполнении работ по техническому обслуживанию средств «закрытого» контура ИС;
- попытки НСД к объектам доступа «закрытого» контура ИС с использованием штатных программно-технических средств «закрытого» контура ИС без нарушения их целостности.

Возможность сговора внутренних нарушителей Н3 и Н4, с персоналом организаций-разработчиков подсистем ИС, а также с внешним нарушителем должна быть исключена применением режимных мер.

2.4.1.1. Описание каналов атак.

Каналами атак являются:

- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
- штатные средства ИС;
- съемные носители информации;
- носители информации, выведенные из употребления;
- штатные программно-аппаратные средства ИС;
- информационные и управляющие интерфейсы СВТ;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- каналы связи вне контролируемой зоны, не защищенные от НСД к информации организационно-техническими мерами;
- каналы, образуемые в результате применения активных радиотехнических методов (АРТМ) (из-за пределов контролируемой зоны);
- каналы распространения побочных электромагнитных излучений и наводок, сопровождающих функционирование технических средств ИС (за пределами контролируемой зоны);
- выходящие за пределы контролируемой зоны цепи инженерно-технических систем (пожаротушения, сигнализации и т.д.), цепи электропитания, цепи заземления, инженерно-технические коммуникации (отопления, водоснабжения и т.д.);
- каналы утечки за счет ЭУНПИ.

2.4.1.2. Описание объектов и целей атак.

К объектам атак (объектам защиты) «закрытого» контура относятся:

- информация, обрабатываемая, передаваемая и хранимая с использованием ТС «закрытого» контура;
- аппаратно-программное обеспечение «закрытого» контура.

Основными целями атак являются:

- нарушение конфиденциальности защищаемой информации (конфиденциальность - защищенность от несанкционированного раскрытия информации об объекте атаки);
- нарушение целостности защищаемой информации (целостность - защищенность от несанкционированной модификации объекта атаки);
- нарушение достоверности защищаемой информации (достоверность - идентичность объекта атаки тому, что заявлено);
- нарушение доступности защищаемой информации (доступность - обеспечение своевременного санкционированного получения доступа к объекту атаки);
- нарушение подконтрольности защищаемой информации. (подконтрольность - обеспечение того, что действия субъекта по отношению к объекту атаки могут быть прослежены уникально по отношению к субъекту).

2.4.1.3.Предположения об имеющихся у нарушителя средствах атак.

Нарушитель может использовать следующие средства атак:

- штатные средства «закрытого» контура ИС;
- доступные в свободной продаже технические, программные и программно-технические средства;
- специально разработанные технические, программные и программно-технические средства;
- средства перехвата и обработки информации в каналах связи, проходящих вне контролируемой зоны, кабельных системах и коммутационном оборудовании, расположенных в пределах контролируемой зоны.

Внешний нарушитель может осуществлять атаки:

- на технические средства ИС (нарушители Н1, Н2);
- на каналы связи, выходящие за пределы контролируемой зоны объектов, на которых располагаются технические средства «закрытого» контура ИС, посредством перехвата секретной информации, последующего ее анализа, уничтожения, модификации, блокирования информации, реализации попыток преодоления системы защиты информации, доступа, навязывания ложной информации и нарушения работоспособности «закрытого» контура ИС в целом и ее отдельных компонент (нарушители Н1).

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

Внутренний нарушитель Н3, может получить физический доступ к техническим средствам, линиям связи, системам электропитания и

заземления при выполнении им обязанностей по регламентному обслуживанию данных средств.

Внутренний нарушитель Н3, может использовать для доступа к защищаемой информации доступные в свободной продаже аппаратные средства и программное обеспечение.

Для реализации доступа к информации, обрабатываемой в «закрытом» контуре ИС, внутренний нарушитель, не являющийся пользователем «закрытого» контура ИС, может располагать:

- компьютером, не имеющим доступа к сети Интернет;
- средствами разработки и отладки программного обеспечения;
- общедоступными компьютерными вирусами.

Возможности внутреннего нарушителя, не являющегося пользователем «закрытого» контура ИС, существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- исключение несанкционированного допуска физических лиц в контролируемую зону и к программно-техническим средствам;
- контроль порядка проведения работ.

Внутренний нарушитель Н3 может осуществлять:

- непреднамеренные (ошибочные) действия при выполнении работ по техническому обслуживанию средств «закрытого» контура ИС;
- попытки НСД к объектам доступа «закрытого» контура ИС с использованием штатных программно-технических средств «закрытого» контура ИС без нарушения их целостности;
- попытки НСД к акустической и визуальной информации «закрытого» контура ИС.

Внутренний нарушитель Н4 и Н5:

- может использовать для доступа к защищаемой информации штатные средства «закрытого» контура ИС и других ведомственных систем;
- обладает возможностями по несанкционированным действиям с использованием штатных средств «закрытого» контура ИС;
- имеет физический доступ к техническим средствам и линиям связи в пределах выделенных ему полномочий, осуществляет легальный доступ к программно-аппаратным средствам и информации со своего рабочего места в соответствии с установленными для него полномочиями, но может пытаться получить доступ к ресурсам «закрытого» контура ИС, выходящий за пределы его полномочий.

2.4.1.4.Описание способов реализации атак «закрытого» контура

Нарушитель может использовать следующие основные способы атак на закрытый «закрытый» контур ИС:

- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей средств защиты, внесенных в процессе разработки этих средств (Н1, Н2, Н3, Н4, Н5, Н6);
- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей средств защиты, внесенных при транспортировке этих средств (Н1, Н2, Н3, Н4, Н5, Н6);
- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей, внесенных при создании и наладке системы защиты (Н1, Н3, Н4, Н5, Н6);
- считывание или восстановление информации (в том числе и фрагментарное) по остаточным следам на носителях защищаемой информации, сданных в ремонт, на обслуживание, переданных для использования другими пользователями или для использования за пределами «закрытого» контура ИС (Н3, Н4, Н5, Н6);
- негласное (скрытое) временное изъятие съемных носителей защищаемой информации, аутентифицирующей или ключевой информации (Н3, Н4, Н5, Н6);
- негласная (скрытая) модификация защищаемой информации, хранящейся на съемных носителях информации (Н4, Н5, Н6);
- визуальный просмотр защищаемой информации на экране монитора (Н3, Н4, Н5, Н6);
- ознакомление с распечатанной защищаемой информацией (Н3, Н4, Н5, Н6);
- вывод информации на неучтенные носители (в том числе, вывод на печать), а также с нарушением требований руководящих и нормативных документов, регламентирующих порядок обращения с информацией соответствующей категории доступа (Н4, Н5, Н6);
- доступ к оставленным без присмотра функционирующим штатным средствам «закрытого» контура ИС (Н3, Н4, Н5, Н6);
- несанкционированное изменение конфигурации технических средств «закрытого» контура ИС (Н6г);
- подбор аутентифицирующей информации пользователей (Н1, Н2, Н5, Н6);
- несанкционированный доступ к защищаемой информации с использованием штатных средств «закрытого» контура ИС (Н4, Н5, Н6);
- модификация ведущихся в электронном виде регистрационных протоколов (журналов регистрации) (Н6);
- модификация технических средств «закрытого» контура ИС (Н6г);
- модификация программных средств «закрытого» контура ИС (Н6);
- вызывание сбоев технических средств «закрытого» контура ИС (Н3, Н4, Н5, Н6);

▪внесение неисправностей в технические средства «закрытого» контура ИС (Н3, Н4, Н5, Н6);

▪блокирование или уничтожение информации, технических, программных и программно-технических компонентов «закрытого» контура ИС СН (Н2, Н3, Н4, Н5, Н6);

▪несанкционированный доступ к защищаемой информации в процессе ремонтных и регламентных работ (Н3);

▪атаки, основанные на использовании уязвимостей и недокументированных (не декларируемых) возможностей технических, программных и программно-технических средств «закрытого» контура ИС, взаимодействующих со средствами защиты и способных повлиять на их функционирование (Н2, Н3, Н4, Н5, Н6).

Перечисленные способы реализации атак нарушителями могут использоваться в различных сочетаниях, направленных на достижение конкретной цели.

Модель нарушителей в «закрытом» контуре приведена на рисунке 2.1.

Рис. 2.1- Модель нарушителей в «закрытом» контуре

2.4.2. Модель нарушителя в «открытом» контуре.

В «открытом» контуре модель нарушителя, как правило, строится с учетом обеспечения только базовой услуги безопасности - **целостность** активов «открытого» контура. Базовые услуги безопасности доступность и конфиденциальность в Модели нарушителя «открытого» контура не рассматриваются.

При разработке модели нарушителя предполагается, что

- внешний нарушитель может проводить атаку только из-за пределов контролируемой зоны;
- для внешнего нарушителя объектом интересов является только информация межсетевого взаимодействия «открытого» контура ИС с «открытыми» контурами ведомственных и других систем. Открытая информация, циркулирующая в «открытом» контуре, не является объектом интересов внешнего нарушителя;
- атаки внешнего нарушителя на «закрытый» «закрытый» контур ИС со стороны открытого контура невозможны;
- атаки на целостность и доступность ресурсов «открытого» контура ИС со стороны внутренних нарушителей (легальных пользователей, эксплуатационно-технического персонала, а также группы нарушителей Н4) не критична с учетом ценности обрабатываемой открытой информации и влияния на функционирование ИС в целом.

В модели нарушителя «открытого» контура ИС, с учетом выше приведенных предположений, должны быть учтены только следующие группы потенциальных нарушителей:

- внешние нарушители (группа Н2);
- внешние нарушители (группа Н7) - субъекты, не имеющий доступа на контролируемую территорию объектов размещения ТС «открытого» контура ИС - пользователи взаимодействующих ведомственных систем, а также пользователи сети Интернет.

2.4.2.1. Предположения об имеющейся у нарушителя информации

Предполагается, что внешний нарушитель:

- обладает общими знаниями по порядку эксплуатации ПСЗИ «открытого» контура ИС (нарушители Н2);
- знает характерные особенности функционирования (технологию использования и структуру) «открытого» контура ИС (нарушители Н2);

Внешний нарушитель может осуществлять атаки:

- на технические средства внешнего взаимодействия «открытого» контура ИС;
- на каналы связи, выходящие за пределы контролируемой зоны объектов ИС, используемые для передачи информации ограниченного доступа, с целью перехвата данной информации и последующего ее анализа, уничтожения, модификации, блокирования доступа к ней, а также реализации попыток преодоления ПСЗИ «открытого» контура ИС, навязывания ложной информации и нарушения работоспособности «открытого» контура ИС в целом и ее отдельных компонент.

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

2.4.2.2. Описание каналов атак

Каналами атак являются:

- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- каналы связи вне контролируемой зоны, не защищенные от НСД к информации организационно-техническими мерами.

2.4.2.3. Описание объектов и целей атак

К *объектам атак* (объектам защиты) «открытого» контура ИС относятся:

- информация межсетевого взаимодействия с сетями сегментов общего пользования, обрабатываемая, передаваемая и хранимая с использованием ТС «открытого» контура ИС;
- аппаратно-программное обеспечение внешней защиты «открытого» контура ИС.

К защищаемой информации относятся:

- информация, используемая при идентификации и аутентификации пользователей при организации межсетевого взаимодействия с сетями сегментов общего пользования;
- ключевая информация межсетевого обмена.

Защищаемые программные и технические средства:

- межсетевые экраны внешнего взаимодействия;
- внешние сервера аутентификации;
- сетевые коммутаторы, маршрутизаторы;
- каналы связи межсетевого взаимодействия «открытого» контура ИС;
- ПО средств внешней защиты информации.

Основными целями атак являются:

- нарушение целостности защищаемой информации в каналах связи общего пользования в процессе межсетевого взаимодействия «открытого» контура ИС с сетями сегментов общего пользования;
- нарушение доступности защищаемой информации;
- нарушение конфиденциальности защищаемой информации.

2.4.2.4. Предположения об имеющихся у нарушителя средствах атак.

Нарушитель может использовать следующие средства атак:

- штатные средства «открытого» контура ИС;
- доступные в свободной продаже технические, программные и программно-технические средства;
- специально разработанные технические, программные и программно-технические средства;
- средства перехвата и обработки информации в каналах связи, проходящих вне контролируемой зоны, кабельных системах и коммутационном оборудовании, расположенных в пределах контролируемой зоны.

Внешний нарушитель может осуществлять атаки:

- на технические средства внешней защиты «открытого» контура ИС (нарушители Н2, Н7);
- на каналы связи, выходящие за пределы контролируемой зоны объектов, на которых располагаются технические средства «открытого» контура ИС (нарушители Н2, Н7).

Возможности внешнего нарушителя (Н4, Н7) существенно зависят от степени защищенности используемых каналов связи (применение криптографических средств защиты, межсетевых экранов, средств обнаружения компьютерных атак и др.).

С учетом особенностей функционирования «открытого» контура и применения средств защиты для противодействия указанным атакам можно предположить, что нарушители (Н4, Н7) относятся к нарушителю, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки. Данный нарушитель является специалистом средней квалификации и для реализации атак не использует недекларированные возможности программных компонент, совместно с которыми предполагается штатное функционирование средств защиты информации «открытого» контура, располагает только доступными в свободной продаже исходными текстами программного обеспечения средств защиты и т. п.

Возможными направлениями действий внешнего нарушителя (Н4, Н7) являются:

- доступ к информации «открытого» контура с целью нарушения ее целостности (модификация информации, в том числе навязывание ложной информации);
- доступ к каналам управления телекоммуникационного и мультипротокольного оборудования межсетевого взаимодействия «открытого» контура с целью постоянного или временного нарушения доступности информации.

Внешний нарушитель (Н4, Н7) может проводить атаку только из-за пределов контролируемой зоны.

Нарушитель (Н4, Н7) может использовать следующие основные способы атак на «открытый» контур:

- перехват разглашаемых сведений об аутентифицирующей или ключевой информации «открытого» контура и ее компонентах, включая средства и систему защиты;
- перехват ключевой информации межсетевого обмена;
- нарушение связи между «открытым» контуром и внешними сегментами сетей общего пользования за счет преднамеренной загрузки трафика ложными сообщениями, приводящей к исчерпанию пропускной способности каналов связи, не защищенных от НСД к информации организационно-техническими мерами.

Модель нарушителя «открытого» контура приведена на рисунке 2.2.

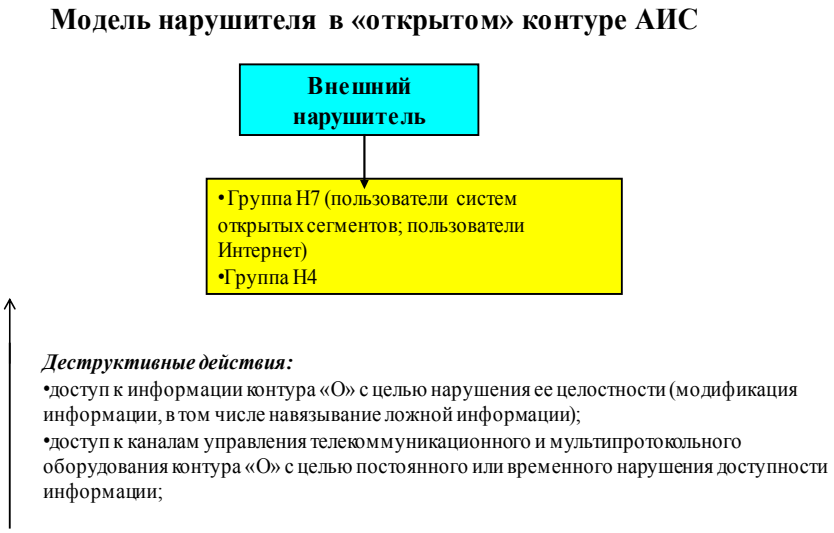

Рис. 2.2 - Модель нарушителя «открытого» контура

2.5. Модели угроз информационной безопасности в ИС

Модель угроз ИБ включает описание источников угрозы, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба. Для источников угроз - людей может быть разработана модель нарушителя ИБ, включающая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий. Модели угроз и нарушителей (прогноз ИБ) должны быть основным инструментом менеджмента хозяйствующих субъектов ИС при развертывании, поддержании и совершенствовании подсистемы ИБ ИС.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями для каждого хозяйствующего субъекта (собственника) сети в отдельности. При анализе угроз ИБ необходимо исходить из того, что эти угрозы непосредственно влияют на операционные риски деятельности указанных субъектов. Операционные риски сказываются на бизнес-процессах ИС. Операционные риски порождаются следующими эксплуатационными факторами: технические неполадки, ошибочные (случайные) и/или преднамеренные злоумышленные действия персонала организации, ее клиентов при их непосредственном доступе к компонентам ИС и другими факторами.

Наиболее эффективным способом минимизации рисков нарушения ИБ для собственника является разработка совокупности мероприятий, методов и средств, создаваемых и поддерживаемых для обеспечения требуемого уровня безопасности информационных активов (подсистемы обеспечения ИБ) в соответствии с политикой ИБ ИС, разрабатываемой в том числе и на основе моделей угроз и нарушителей ИБ.

При построении ПИБ ИС, в первую очередь необходимо определить какие угрозы должны быть устранены и в какой мере, какие ресурсы ИС должны быть защищены и в какой степени, а также – с помощью каких механизмов должна быть реализована защита и оценка затрат на ее реализацию и эксплуатацию средств защиты.

2.5.1. Общее описание угроз информационное безопасности.

Под угрозами безопасности информационных и программных активов ИС понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение активов, а также иных несанкционированных действий при их обработке в ИС.

Угрозы безопасности информации реализуются действиями нарушителя, которые могут предприниматься им с целью проведения атак на компоненты ИС. При этом атаки определены, если определены объект, цель, канал и способ нападения, а также средства нападения.

Под уровнем угрозы понимается вероятность ее осуществления. Оценка уязвимостей предполагает определение вероятности успешного осуществления угроз безопасности. Успешное осуществление угрозы означает нанесение ущерба активам «закрытого» контура. Наличие уязвимостей в «закрытом» контуре обусловлено слабостями защиты. Таким образом, вероятность нанесения ущерба определяется вероятностью осуществления угрозы и величиной уязвимости. Величина риска определяется на основе стоимости актива, уровня угрозы и величины уязвимости. С увеличением стоимости актива, уровня угрозы и величины уязвимости возрастает и величина риска. На основе оценки величины рисков определяются требования безопасности.

Угрозы безопасности информации для «закрытого» контура вытекают из модели нарушителя «закрытого» контура и технологии обработки секретной информации в «закрытом» контуре.

Все угрозы для защищаемой в «закрытом» контуре ИС информации подразделяются на два класса:

- угрозы, не являющиеся атаками;
- атаки.

Под атакой понимается целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью

нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.

Существуют угрозы, которые не являются атаками, но которые могут не только привести к потере, искажению или компрометации защищаемой информации, но и создать условия, которые может использовать в своих целях нарушитель.

К таким угрозам относятся:

- угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.);
- угрозы социально–политического характера: забастовки, саботаж, локальные конфликты, сопровождаемые нападением на объект, в котором размещаются ресурсы «закрытого» контура ИС СН, и т.д.;
- ошибочные действия и (или) нарушения требований эксплуатационной и другой документации персоналом и пользователями «закрытого» контура ИС СН, к которым, в частности, относятся:

а. непредумышленное искажение или удаление программных компонентов;

б. внедрение и использование неучтенных программ;

в. игнорирование организационных ограничений (установленных правил) при работе с ресурсами «закрытого» контура ИС СН, включая средства защиты информации, в частности:

д. нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);

е. предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требованиям;

ж. настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

и. несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

к. угрозы техногенного характера, основными из которых являются:

л. аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т. д.);

м. неисправности, сбои аппаратных компонентов средств «закрытого» контура ИС СН, нестабильность параметров системы электропитания, заземления и т. д.;

н. помехи и наводки, приводящие к сбоям в работе аппаратных компонентов средств «закрытого» контура ИС СН.

Основными целями атак в «закрытом» контуре являются:

▪нарушение конфиденциальности защищаемой информации (конфиденциальность - защищенность от несанкционированного раскрытия информации об объекте атаки);

▪ нарушение целостности защищаемой информации (целостность - защищенность от несанкционированной модификации объекта атаки);

▪ нарушение достоверности защищаемой информации (достоверность - идентичность объекта атаки тому, что заявлено);

▪ нарушение доступности защищаемой информации (доступность - обеспечение своевременного санкционированного получения доступа к объекту атаки).

Угрозы безопасности информационных ресурсов, сточки зрения реализации, можно разделить на следующие группы:

- Угрозы, реализуемые с использованием технических средств;
- Угрозы, реализуемые с использованием программных средств;
- Угрозы, реализуемые путем использования технических каналов утечки информации.

2.5.1.1. Угрозы, реализуемые с использованием технических средств

Общее описание

Технические средства системы включают в себя приемо-передающее и коммутирующее оборудование, оборудование серверов и рабочих станций, а также линии связи. К данному классу относятся угрозы доступности, целостности и, в некоторых случаях конфиденциальности информации, хранимой, обрабатываемой и передаваемой по каналам связи системы, связанные с повреждениями и отказами технических средств ИС, приемо-передающего и коммутирующего оборудования и повреждением линий связи.

Виды угроз

Для технических средств характерны угрозы, связанные с их умышленным или неумышленным повреждением, ошибками конфигурации и выходом из строя:

- Вывод из строя (умышленный или неумышленный);
- Несанкционированное либо ошибочное изменение конфигурации активного сетевого оборудования и приемо-передающего оборудования;
- Физическое повреждение технических средств, линий связи, сетевого и каналообразующего оборудования;
- Перебои в системе электропитания;
- Отказы технических средств;
- Установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты;
- Хищение технических средств и долговременных носителей конфиденциальной информации вследствие отсутствия контроля над их использованием и хранением.

Источники угроз.

В качестве источников угроз безопасности для технических средств системы выступают как внешние и внутренние нарушители, так и природные явления. Среди источников угроз для технических средств можно отметить:

- стихийные бедствия;
- пожар;
- кража оборудования;
- саботаж;
- ошибки обслуживающего персонала;
- терроризм и т. п.

2.5.1.2. Угрозы, реализуемые с использованием программных средств

Общее описание

Это наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов, связанный с получением НСД к информации, хранимой и обрабатываемой в системе, а также передаваемой по каналам связи, при помощи использования возможностей, предоставляемых ПО ИС. Большинство рассматриваемых в этом классе угроз реализуется путем осуществления локальных или удаленных атак на информационные ресурсы системы внутренними и внешними злоумышленниками. Результатом успешного осуществления этих угроз становится получение НСД к информации БД и файловых систем корпоративной сети, данным, хранящимся на АРМ операторов, конфигурации маршрутизаторов и другого активного сетевого оборудования.

Виды угроз

В этом классе рассматриваются следующие основные виды угроз:

- Внедрение вирусов и других разрушающих программных воздействий;
- Нарушение целостности исполняемых файлов;
- Ошибки кода и конфигурации ПО, активного сетевого оборудования;
- Анализ и модификация ПО;
- Наличие в ПО недекларированных возможностей, оставленных для отладки, либо умышленно внедренных;
- Наблюдение за работой системы путем использования программных средств анализа сетевого трафика и утилит ОС, позволяющих получать информацию о системе и о состоянии сетевых соединений;
- Использование уязвимостей ПО для взлома программной защиты с целью получения НСД к информационным ресурсам или нарушения их доступности;
- Выполнение одним пользователем несанкционированных действий от имени другого пользователя («маскарад»);
- Раскрытие, перехват и хищение секретных кодов и паролей;
- Чтение остаточной информации в ОП компьютеров и на внешних носителях;
- Ошибки ввода управляющей информации с АРМ операторов в БД;
- Загрузка и установка в системе не лицензионного, непроверенного системного и прикладного ПО;

- Блокирование работы пользователей системы программными средствами.

Отдельно следует рассмотреть угрозы, связанные с использованием сетей передачи данных. Данный класс угроз характеризуется получением внутренним или внешним нарушителем сетевого доступа к серверам БД и файловым серверам, маршрутизаторам и активному сетевому оборудованию. Здесь выделяются следующие виды угроз, характерные для КСПД предприятия:

- перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика;
- замена, вставка, удаление или изменение данных пользователей в информационном потоке;
- перехват информации (например, пользовательских паролей), передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации;
- статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т. п.).

Источники угроз

В качестве источников угроз безопасности для технических средств системы выступают как внешние и внутренние нарушители.

2.5.1.3. Угрозы утечки информации по техническим каналам связи

Виды технических каналов утечки информации

При проведении работ с использованием конфиденциальной информации и эксплуатации технических средств ИС возможны следующие каналы утечки или нарушения целостности информации или работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- несанкционированный доступ к информации, обрабатываемой в автоматизированных системах;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств.

Наибольшую опасность в настоящее время представляют технические средства разведки:

- Акустическая разведка;

- Разведка побочных электромагнитных излучений и наводок электронных средств обработки информации (далее - ПЭМИН);
- В отдельных ситуациях, могут использоваться: телевизионная, фотографическая и визуальная оптическая разведка, обеспечивающая добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне электромагнитных волн с использованием телевизионной аппаратуры.

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание конфиденциальной информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Утечка информации возможна по следующим каналам:

- Радиоканалы;
- ИК-канал;
- Ультразвуковой канал;
- Проводные линии.

В качестве проводных линий при передаче информации к внешним средствам регистрации могут быть использованы:

- сети переменного тока;
- линии телефонной связи;
- радиотрансляционные и технологические (пожарной, охранной сигнализации, кабели телеантенн и т.п.) линии;
- специально проложенные проводные линии.

При применении лазерной аппаратуры дистанционного прослушивания, фиксирующей информативные колебания стекол в окнах помещений, возможен съем акустической информации из выделенных помещений, в которых установлены элементы системы.

Источники угроз

В качестве источников угроз безопасности для технических средств системы выступают как внешние и внутренние нарушители, оснащенные специализированными средствами технической разведки.

Основные внешние угрозы защищаемым ресурсам ИС:

- атаки на информационные ресурсы ИС;
- катастрофы и неблагоприятные события природного и техногенного характера;
- террористические акты;
- зависимость от монопольных поставщиков аппаратно-программных и технических средств, расходных материалов, телекоммуникационных услуг и т.п.;
- атаки из внешних информационных сред на аппаратно-программные и технические комплексы ИС .

Основные внутренние угрозы защищаемым ресурсам ИС предприятия:

- невыполнение сотрудниками ИС установленных технических и/или технологических регламентов;

- несанкционированная деятельность (включая ошибки) персонала и пользователей автоматизированных систем и МСС, приводящая к изменению настроек оборудования, аппаратно-программных средств и комплексов, влияющих на информационную безопасность;
- несанкционированное использование информационных ресурсов (чтение, копирование, публикация, искажение, уничтожение, ввод ложной информации и т.п.).

Функционирование ИС поддерживается входящей в ее состав инфраструктурой, которая обеспечивает реализацию инфокоммуникационных технологий и может быть представлена в виде иерархии следующих основных уровней:

- физической среды (линии связи, аппаратные средства и пр.);
- области взаимодействия (канальные и сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
- приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- технологических процессов;
- бизнес-процессов операторов ИС.

На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными. Главной целью злоумышленника является получение контроля над активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например, путем раскрытия конфиденциальной информации, более эффективно для злоумышленника и опаснее для собственника инфоуслуг, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т. ч. временных) и поэтому менее эффективное по соотношению «затраты/получаемый результат». Хозяйствующие субъекты ИС должна определить конкретные объекты защиты на каждом из уровней информационной инфраструктуры.

Наиболее актуальные источники угроз на уровнях физической среды, области взаимодействия и уровне приложений:

- внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры, фрикеры и иные лица, осуществляющие несанкционированный доступ (НСД);
- внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе, сетевому, администраторы сетевых приложений и т.п.);
- комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных и технологических процессов:

- внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи приложений инфоуслуг, технического обслуживания и управления, администраторы ИБ и т.д.);
- комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

Наиболее актуальные источники угроз на уровне бизнес-процессов:

- внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АСИ, представители менеджмента организации и пр.);
- комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

Кроме того, также необходимо учитывать угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью.

Совокупность возможных угроз со стороны потенциального злоумышленника с учетом имеющихся в его распоряжении сил и средств на некотором интервале времени образуют модель защиты политики ИБ ИС. Модель защиты — это некоторая упорядоченная совокупность всей доступной информации о возможных угрозах и условиях осуществления утрат со стороны потенциального злоумышленника, наносимом ущербе правовой оболочке (среде), в которой действуют злоумышленник и информационная технология, защитных свойствах технологии и используемых в ней средств защиты информации.

2.5.2. Модели угроз «закрытого» контура

Основные угрозы нарушения **конфиденциальности** в «закрытом» контуре:

- ознакомление с секретными данными, хранимыми или обрабатываемыми в базах данных «закрытого» контура, лиц, не допущенных к данным сведениям;
- НСД к АРМ пользователя и нелегальное использование нарушителем прав легального пользователя;
- несанкционированный доступ к информации, выводимой на устройства отображения;
- действия вредоносных программ и вирусов;
- компрометация ключевой информации подсистемы криптографической защиты информации «закрытого» контура;
- нарушение регламента выполнения работ;
- ошибки администрирования;
- создание неучтенных, незаконных копий информационных массивов;
- хищение носителей секретной информации (магнитных дисков, лент, запоминающих устройств и целых ПЭВМ;

- перехват административных паролей серверов и сетевого оборудования с помощью прослушивания сети;
- перехват побочных электромагнитных излучений и наводок АРМ пользователей на вспомогательные технические средства и системы (ВТСС), непосредственно не участвующие в обработке секретной информации, но размещаемые совместно с АРМ пользователей;
- перехват сигналов акустоэлектрических преобразований АРМ пользователей «закрытого» контура и ВТСС, размещаемых в выделенных помещениях ВП;
- перехват обрабатываемой на АРМ пользователей «закрытого» контура секретной информации по цепям электропитания и системе заземления методом ВЧ-навязывания;
- перехват секретной информации из защищаемых помещений «закрытого» контура и установленных ТС за счет ЭУНПИ;
- перехват секретной акустической речевой информации по ТКУИ, в том числе при использовании активных радиотехнических методов.
- несанкционированный доступ к ТС «закрытого» контура внутренних нарушителей, не являющихся пользователями «закрытого» контура;
- внедрение аппаратных или программных «закладок» и «вирусов» с целью регистрации и передачи защищаемой секретной информации или дезорганизации функционирования «закрытого» контура;
- перехват секретной информации за счет использования ЭУНПИ;
- перехват обрабатываемой секретной информации по цепям электропитания и системе заземления, в том числе методом ВЧ-навязывания;
- перехват секретной информации за счет использования ЭУНПИ;
- перехват IP-соединений и работа от имени администратора или пользователя «закрытого» контура;
- генерация фальшивых управляющих ICMP-пакетов для изменения параметров маршрутизации;
- использование слабых мест в сетевых службах для взлома сетевых ресурсов «закрытого» контура;
- использование слабых мест системы доменных имен DNS для формирования ложных таблиц хостов «закрытого» контура;
- использование протокола SNMP управления ЛВС «закрытого» контура для получения сведений о сетевом оборудовании и возможного перехвата и подмены управляющих сетевых сообщений;
- удаленные атаки на средства защиты от НСД и средства криптографической защиты информации с целью нарушения их работы;
- неквалифицированные или неправомерные действия администраторов систем защиты информации, приводящие к нарушению работы этих систем и др.;

2.5.2.1. Значимые угрозы нарушения конфиденциальности

Для серверов ИС:

Ознакомление с конфиденциальными данными, хранимыми или обрабатываемыми в системе, лиц, не допущенных к данным сведениям;
Создание неучтенных, незаконных копий информационных массивов;
Хищение носителей информации (магнитных дисков, лент, запоминающих устройств и целых ПЭВМ), производственных отходов (распечаток, записей, списанных носителей информации и т.п.).
Для системы передачи данных:
Перехват административных паролей паролей серверов и сетевого оборудования с помощью прослушивания сети (сниффинга);
Перехват конфиденциального трафика с помощью сниффинга;
Использование захвата IP-соединений и работы вместо администратора или пользователя (технологии спуффинга);
Генерация фальшивых ICMP-пакетов для изменения параметров маршрутизации;
Использование слабых мест в сетевых службах для взлома сетевых ресурсов;
Использование слабых мест системы DNS для формирования ложных таблиц хостов;
Использование слабых мест почтовой системы для взлома почтовой машины;
Использование протокола SNMP управления сетью для получения сведений о сетевом оборудовании и возможного перехвата и подмены управляющих сетевых сообщений;
Подбор паролей;
Занесение вируса с почтовой корреспонденцией.

Для систем защиты от НСД и средств криптографической защиты информации:
Компрометация ключевой информации систем криптографической защиты информации;
Дешифрование защищенной криптографическими методами информации с помощью методов криптоанализа.

Нарушение **конфиденциальности** может привести к несанкционированному предоставлению привилегий пользователям СУБД и ОС, что может повлечь доступ и искажение информации в «закрытом» контуре и служебной информации файлов аудита СУБД и ОС «закрытого» контура, а так же к разглашению или утечке секретной информации из «закрытого» контура. Нарушитель, поразив конфиденциальность компонент «закрытого» контура (например, перехватив административные пароли) может исказить какой либо конфигурационный файл и тем самым осуществить атаку на целостность и доступность системы.

*2.5.2.2. Значимые угрозы нарушения **целостности** данных и программных ресурсов*

Основные угрозы нарушения **целостности** программ и данных «закрытого» контура:

- несанкционированное изменение БД прикладных задач «закрытого» контура;
- несанкционированное изменение компонентов ОС и СУБД, а также программного обеспечения приложений «закрытого» контура;
- несанкционированное изменение операционной среды АРМ пользователей «закрытого» контура;
- несанкционированные действия нарушителя от имени легального пользователя «закрытого» контура, носящие деструктивный характер или приводящие к искажению информации;
- изменения конфигурации и режимов функционирования серверов «закрытого» контура;
- внесение несанкционированных изменений в настройки коммуникационного оборудования «закрытого» контура.
- сбои оборудования;
- физическое воздействия;
- преднамеренные действия легальных пользователей по нарушению функционирования системы или преодолению механизмов защиты «закрытого» контура;
- ошибки в системном и программном обеспечении;
- вирусные воздействия.

К ***значимым угрозам***, приводящим к нарушению целостности программ и данных необходимо отнести:

Для серверов ИС:

- Несанкционированное изменение базы данных ИС;
- Несанкционированное изменение компонентов ОС и СУБД, а также ПО ИС;
- Несанкционированное изменение операционной среды АРМ, действия нарушителя в среде ИС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению платежной информации.

Для АРМ:

- Несанкционированное изменение операционной среды АРМ, действия нарушителя в среде ИС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению платежной информации.

Для ОС ЛВС:

- изменения конфигурации и режимов функционирования файлового сервера ЛВС.

Для корпоративной сети:

- Внесение несанкционированных изменений в настройки коммуникационного оборудования.

Нарушение **целостности** данных, а также программных компонентов, находящихся как на сервере, так и на рабочих станциях «закрытого» контура

может привести к некорректному функционированию ПО и преодолению системы защиты. Нарушитель, поразив целостность компонент «закрытого» контура, может заблокировать ее нормальное функционирование и тем самым осуществить атаку на доступность системы.

Средства поддержания целостности разделяются на две группы: средства контроля целостности и средства восстановления целостности после её нарушения. С помощью этих средств решаются следующие основные задачи:

- обеспечение целостности программ и обрабатываемых данных;
- обеспечение целостности сообщений при передаче информации по каналам связи;
- обеспечение целостности архивной информации;
- обеспечение целостности системы защиты.

Основные угрозы нарушения **доступности** активов «закрытого» контура:

- удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании» (Denial of Service), использование возможных уязвимостей сервисов);
- локальные атаки на систему защиты ОС внутренним легальным пользователем «закрытого» контура (подбор паролей, использование возможных уязвимостей файловой системы, настроек сервисов и драйверов) с целью нарушения работы серверов приложений «закрытого» контура;
- неквалифицированные или неправомерные действия администраторов ОС и СУБД «закрытого» контура, приводящие к нарушению работы прикладных задач;
- изменения конфигурации ОС АРМ пользователей ЛВС «закрытого» контура (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС и др.);
- удаление (модификации) исполняемых файлов прикладного и системного программного обеспечения;
- внесение компьютерных вирусов;
- внедрение программ, осуществляющих некорректные действия в АСИ, из-за имеющихся в них ошибок или специальных программных «закладок»;
- внесение модификаций в ПО системы управления ЛВС «закрытого» контура, приводящих к дезорганизации функционирования АРМ пользователей «закрытого» контура;
- вывод из строя или изменение конфигурации сетевого оборудования «закрытого» контура, приводящее к потери доступа к сетевым ресурсам;
- проявление ошибок программно-аппаратных средств «закрытого» контура;
- некомпетентное использование и настройка средств защиты;
- случайный ввод ошибочных данных;

- искажение регистрационных данных;
- действия вредоносных программ;
- неправомерное включение, выключение оборудования или изменение режимов работы устройств и программ;
- повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на функционирование сервисов безопасности «закрытого» контура.

*2.5.2.3. Значимые угрозы нарушения **доступности** информационных, программных и аппаратных ресурсов*

Для северов ИС (ОС и СУБД):

Удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа “отказ в обслуживании” - Denial of Service, использование уязвимостей сервисов);

Локальные атаки на систему защиты ОС легальным пользователем (подбор паролей, использование уязвимостей файловой системы, настроек сервисов и драйверов) с целью нарушения работы серверов ИС;

Неквалифицированные или неправомерные действия администраторов ОС и СУБД, приводящие к нарушению работы ИС.

Для АРМ:

изменения конфигурации ОС (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС для Windows);

удаления (модификации) исполняемых файлов прикладного и системного программного обеспечения;

внесения компьютерных вирусов;

эксплуатации программ, осуществляющих некорректные действия, из-за имеющихся в них ошибок или специальных "закладок".

Для ОС ЛВС:

Удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки Denial of Service, использование уязвимостей сервисов);

Внесение модификаций в ПО, хранящееся на серверах ЛВС, приводящих к дезорганизации функционирования АРМ ползователя.

Для системы передачи данных:

Вывод из строя или изменение конфигурации сетевого оборудования, приводящее к потери доступа к сетевым ресурсам.

Для систем защиты от НСД и средств криптографической защиты информации:

Удаленные атаки на средства защиты от НСД и средства криптографической защиты информации с целью нарушения их работы;

Неквалифицированные или неправомерные действия администраторов систем защиты информации, приводящие к нарушению работы этих систем.

Нарушения **доступности** информационных, программных и аппаратных ресурсов может привести к дезорганизации процесса обработки информации (несанкционированный останов СУБД, ОС, уничтожение данных и так далее).

Предполагается, что защита от угроз, не являющихся атаками, в основном регламентируется инструкциями, разработанными и утвержденными подразделениями, эксплуатирующими различные компоненты «закрытого» контура ИС с учетом особенностей эксплуатации этих компонентов и действующей нормативной базы.

Кроме этого, большинству угроз, не являющихся атаками, можно сопоставить атаки, и защита от такого рода угроз должна обеспечиваться средствами защиты информации, входящими в подсистему информационной безопасности «закрытого» контура ИС СН и разрабатываемыми в основном с целью противодействия атакам.

2.5.3. Модели угроз в «открытом» контуре

Угрозы нарушения целостности и/или доступности информации «открытого» контура:

- удаленные атаки на сетевые сервисы «открытого» контура с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании», использование уязвимостей сервисов);
- повреждение каналов связи;
- действия, приводящие к частичному или полному отказу сетевого оборудования и средств сетевого управления «открытого» контура;
- неправомерная модификация передаваемых данных, технической и служебной информации.

Угрозы нарушения конфиденциальности информации «открытого» контура:

- незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа (включая получение аутентифицирующей и ключевой информации для его последующего неправомерного использования) и т.п.;
- незаконное подключение к сетевому оборудованию с целью изменения настроек и анализа проходящего потока данных и служебного трафика;
- воздействие на внешнее сетевое оборудование «открытого» контура, приводящее к его некорректному функционированию (неправильной фильтрации, адресации информации и т.п.);
- использование уязвимостей интерфейсов и протоколов взаимодействия оборудования «открытого» контура.

2.6. Определение перечня требований информационной безопасности