ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Н. Н. Мошак
Л.К. Птицына

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УЧЕБНОЕ ПОСОБИЕ

САНКТ-ПЕТЕРБУРГ
2020

УДК 004.056

Рецензенты: доктор технических наук, профессор В.А. Богатырев
доктор технических наук, профессор А.Н. Молдовян

Утверждено редакционно-издательским советом СПбГУТ
в качестве учебного пособия

Мошак, Н. Н., Защищенные информационные системы: учебное пособие / Н. Н. Мошак, Л. К. Птицына; СПбГУТ. – СПб., 2020. – 225 с.

Приводятся общие подходы к обеспечению безопасности информационных систем. Основное внимание уделяется построению политики информационной безопасности корпоративной информационной системы (ИС) на базе архитектуры «клиент-сервер». Описываются модели нарушителей, угрозы информационной безопасности ИС, формулируются требования информационной безопасности. Приводитсякомплекс организационно-технических мер по реализации требований информационной безопасности и контроля уровня защиты.

Излагаются процессные подходы (принципы) управления информационной безопасностью ИС на базе модели Д. Деминга. Анализируются основные процедуры этапов жизненного цикла системы управления информационной безопасности организации.

Предназначено для подготовки бакалавров и магистров 10.04.01 и 10.03.01 по направлениям «Информационная безопасность». Профиль – Безопасность компьютерных систем.

УДК 004.056

Введение

Информация – самый ценный ресурс организации, от безопасности которого зависят технологические и бизнес-процессы. По мере развития информационных технологий возрастает риск утечки информации, заражения вирусом, несанкционированного вмешательства в информационные системы организации. Информационная система (ИС) – это взаимосвязанный набор инструментов, способов и персонала, которые используются для хранения, обработки, передачи и приема информации для достижения цели.

Объектом защиты в данном руководстве является ИС организации.

Предметом защиты в ИС является информация.

Информационная безопасность (ИБ) ИС организации – указанная вероятность безопасности ее активов (информации и программного обеспечения, технических средств, сотрудников, имиджа организации) с учетом приоритетов служб защиты, модели угрозы и нарушителя.

Цель ИБ в ИС организации – снизить размер вероятного ущерба до допустимых значений, а также надежно и качественно эксплуатировать его в условиях возникающих угроз.

Информационные системы, в которых обеспечивается безопасность информации, называются защищенными.

Защищенность ИС достигается проведением руководством организации соответствующей политики информационной безопасности (далее - Политика), требования которой являются основой для построения системы информационной безопасности (СИБ) организации. Одноименный документ разрабатывается и принимается как официальный Р Д организации в части ИБ ИС. *Политика ИС определяет,* ***что нужно защищать.*** Поэтому после определения официальной Политики следует определить конкретные защитные меры и средства, а также меры контроля, реализующие практические процедуры защиты.

Процедуры защиты определяют, ***как именно выполнять и контролировать требования Политики ИС.*** Конкретные меры защиты реализует СИБ организации– единый комплекс правовых норм, организационных и технических мер, обеспечивающий защищенность информации в соответствии с принятой Политикой. СИБ, как процесс защиты, относится к вспомогательным процессам, обеспечивающий качество основного бизнес-процесса организации. Процедуры оперативного контроля состояния и управления ИБ реализует система управления ИБ (СУИБ) организации. СУИБ – часть менеджмента (скоординированной деятельности по руководству и управлению) организации, предназначенного для создания, эксплуатации, мониторинга, анализа и совершенствования системы обеспечения ИБ (СОИБ) организации.

Таким образом, СОИБ организации объединяет как систему информационной защиты СИБ, так и систему управления – СУИБ.

Защита информации – комплекс мероприятий, направленных на обеспечение ИБ организации, которая основывается на законодательстве Российской Федерации, Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000г. [1], государственных законах в области ИБ [2-5], государственных нормативно-методических документах в области ИБ (государственных стандартах [6-10], руководящих документах (РД) Федеральной службы по техническому и экспортному контролю (ФСТЭК) [11-14], Министерства обороны РФ, Федеральной службы безопасности РФ, Мининформсвязи РФ), а также организации.

Глава 1. Политика информационной безопасности организации

1.1. Основные этапы построения политики информационной безопасности

В основе безопасности организации и в первую очередь безопасности ее информационной системы (ИС) лежит политика информационной безопасности (далее – Политика) [15-17]. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению информационной безопасности 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 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. Политика 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;

–разработка модели нарушителя ИБ и модели угроз ИБ;

– определение перечня требований ИБ ИС;

– разработка организационно-технических предложений по методам и механизмам защиты ИС организации;

– разработка организационно-технических требований по мониторингу и контролю эффективности ИБ организации.

1.2. Структура объекта защиты

Корпоративная ИС представляет собой совокупность территориально разнесенных объектов, между которыми осуществляется информационный обмен.

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 (рис.1.1).

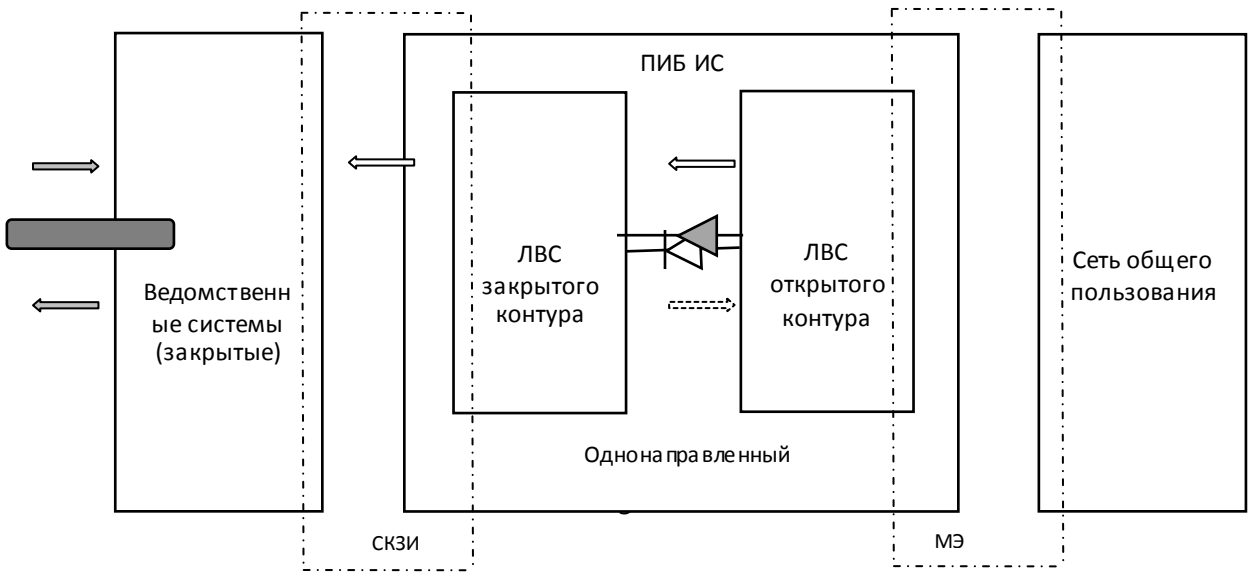

Рис. 1.1. Обобщенная схема информационных потоков в ИС

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». 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.

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

– серверы СУБД и файл-серверы «закрытого» и «открытого» контуров, осуществляющие обработку и хранение информации;

– автоматизированные рабочие места (АРМ) пользователей «закрытого» и «открытого» контуров ИС;

– корпоративную мультисервисную сеть связи (МСС) на основе IP-QoS технологий, включающая в себя защищенную WAN-компоненту, обеспечивающую связь территориально удаленных локальных вычислительных сетей (ЛВС) «закрытых» контуров. В корпоративную сеть входят структурированные кабельные системы (СКС), на базе которых строятся ЛВС «закрытого» и «открытого» контуров, сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.) и внешние защищенные каналы связи. Связь территориально удаленных «открытых» контуров ЛВС осуществляется по сетям связи общего пользования (Интернет, LTE и др.) с использованием технологии VPN.

1.2.1. Эволюция классической архитектуры «клиент-сервер» информационных систем

Различают несколько моделей архитектуры «клиент-сервер», каждая из которых отражает соответствующее распределение компонентов программного обеспечения между компьютерами сети по функциональному признаку [17,18].

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:

– компоненты представления (presentation), реализующей интерфейс с пользователем;

– прикладной компоненты (business application), обеспечивающей выполнение прикладных функций;

– компоненты доступа к информационным ресурсам (resource access) или менеджера ресурсов (resource manager), выполняющей накопление информации и управление данными.

В архитектуре «клиент/сервер» функции приложения распределены между двумя (или более) компьютерами. Укажем модели архитектуры «клиент-сервер», соответствующие типам распределения перечисленных компонентов между рабочей станцией и сервером сети:

Фундаментальное различие между моделями архитектуры «клиент—сервер» заключается в следующем. Модели доступа к удаленным данным (рис.1.2) и модели сервера базы данных (рис.1.3) опираются на двухзвенную схему разделения функций.

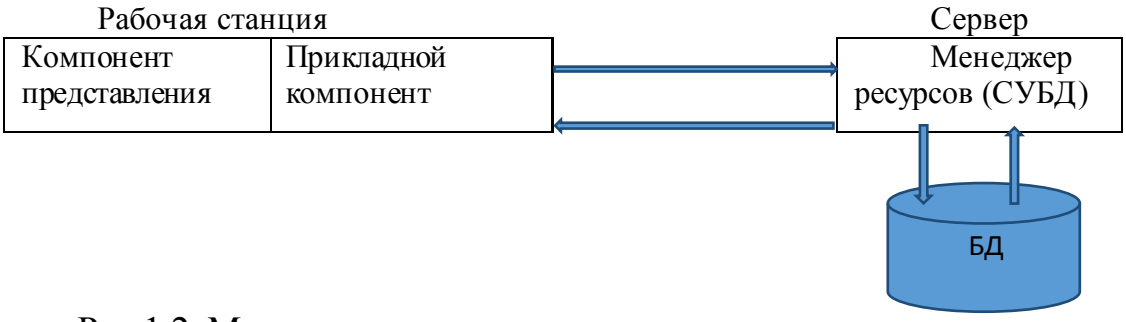

Рис.1.2. Модель доступа к удаленным данным

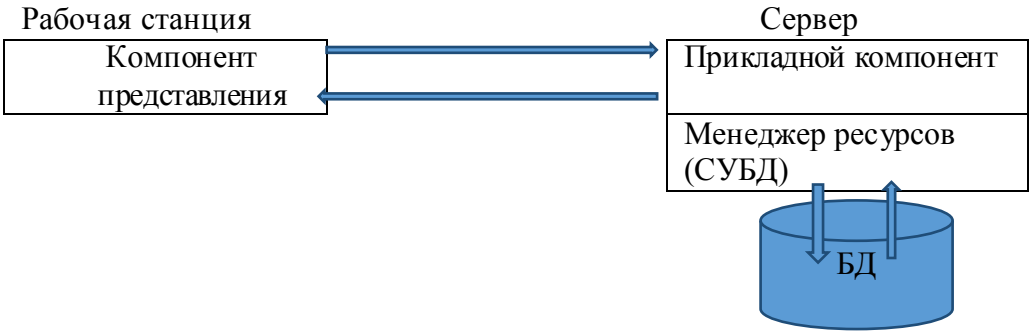

Рис.1.3. Модель сервера управления данными

В модели доступа к удаленным данным прикладные функции приданы программе—клиенту, в модели сервера базы данных ответственность за их

выполнение берет на себя ядро СУБД. В первом случае прикладная компонента сливается с компонентом представления, во втором - интегрируется с компонентой доступа к информационным ресурсам. Напротив, в модели сервера приложений (рис.1.4) реализована классическая трехзвенная схема разделения функций, где прикладная компонента выделена как важнейший элемент приложения.

Рис. 1.4. Трехзвенная архитектура «клиент-сервер»

Для ее определения используются универсальные механизмы многозадачной операционной системы, и стандартизованы интерфейсы с двумя другими компонентами. Собственно, из этой особенности модели сервера приложений и вытекают ее преимущества.

Особенности классической сетевой архитектуре «клиент-сервер»:

– 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.

Последняя особенность способствует повышению информационно-компьютерной безопасности, т. к. исключается миграция программ по сети при обработке серверами запросов со стороны клиентов и снижается вероятность запуска на выполнение вредоносных программ и заражения компьютерными вирусами.

С точки зрения безопасности обработки и хранения данных архитектура «клиент-сервер» обладает рядом недостатков:

– территориальная распределенность компонент программных приложений и неоднородность элементов вычислительной системы приводят к существенному усложнению построения и администрирования системы информационной безопасности;

– часть защищаемых информационных ресурсов может располагаться на автоматизированных рабочих местах (АРМ) оператора или рабочих станциях (РС), которые характеризуются повышенной уязвимостью;

– использование для обмена данными между компьютерами сети закрытых протоколов требует разработки уникальных средств защиты и соответственно повышенных затрат;

– при потере параметров настройки программного обеспечения какого-либо АРМ необходимо выполнение сложных процедур связывания и согласования этого АРМ с остальной частью вычислительной системы, что приводит к увеличению времени восстановления работоспособности компьютерной сети при возникновении отказов.

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

Многие недостатки, присущие компьютерным сетям с классической архитектурой «клиент-сервер», отсутствуют в новой архитектуре компьютерных сетей, названной *Intranet—архитектурой* или *Web—архитектурой*, или архитектурой «клиент-сервер», основанной на *Web—технологии*. Базисом новой архитектуры является Web—технология. В соответствии с Web—технологией на сервере размещаются так называемые Web—документы, которые визуализируются и интерпретируются программой навигации, функционирующей на рабочей станции (рис. 1.5).

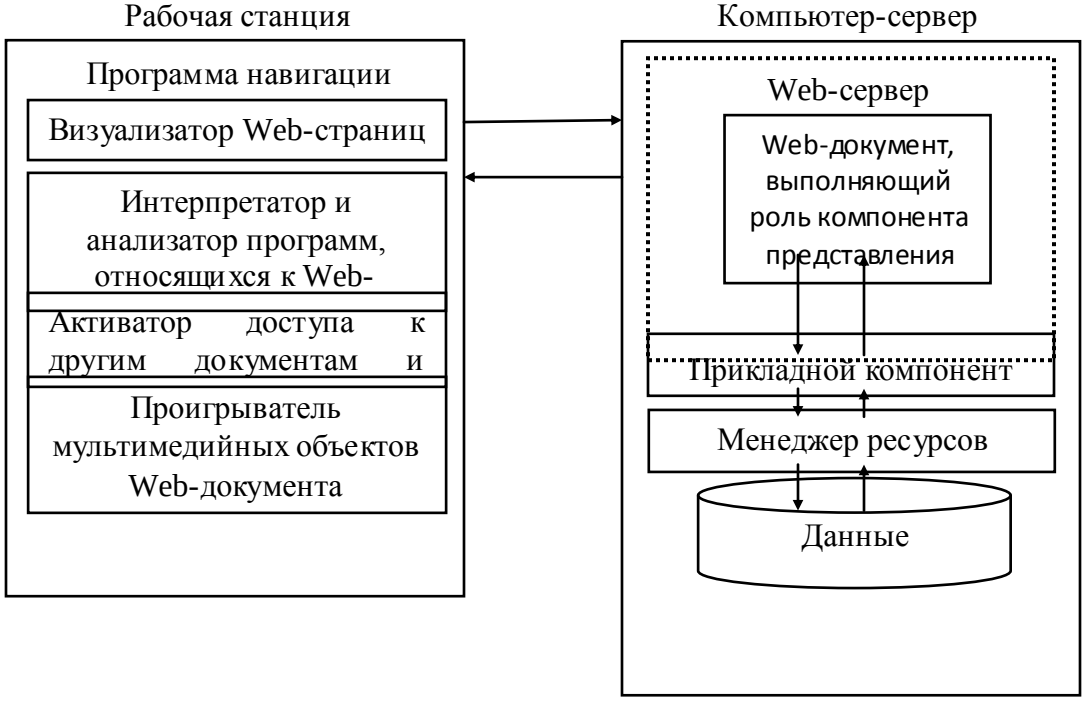

Рис.1.5. Архитектура «клиент-сервер», основанная на Web-технологии

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.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. 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. Можно выделить следующие отличительные черты Intranet—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.

Отметим, что важным плюсом использования серверов баз данных является возможность встроить развитую систему безопасности сервера в систему безопасности информационной системы. В частности, серверы 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. 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. Не нужно решать задачу обеспечения безопасного информационного взаимодействия для множества приложений каждого компьютера. Решение по безопасности взаимодействия для одного компьютера и будет стандартным для всех. Кроме того, по отношению к протоколам открытого стандарта намного интенсивнее и шире публичное обсуждение вопросов информационной безопасности и богаче выбор защитных средств. Облегченное централизованное управление сервером и компьютерами-клиентами снижает вероятность допущения непреднамеренных ошибок пользователями, операторами и администраторами. Однако возможность выполнения на АРМ программ с сервера порождает новые угрозы безопасности информации, например, появляется угроза подмены передаваемой с сервера программы. Соответственно возможность миграции программ предъявляет дополнительные требования по поддержанию безопасности сетевого взаимодействия.

Таким образом, модель доступа к удаленным данным является оптимальным решением при построении небольших информационных систем, в которых не требуется графический интерфейс с пользователем. В случае необходимости использования графического интерфейса можно ориентироваться на модель сервера управления данными архитектуры «клиент/сервер». Модель трехзвенной архитектуры «клиент/сервер» является лучшим вариантом для создания больших информационных систем, а также в случае использования низкоскоростных каналов связи. В пределах одной информационной системы ее составные части, в принципе, могут быть построены с использованием различных архитектур. Например, часть рабочих мест пользователей, на которых происходит ввод данных в систему, может функционировать в режиме модели доступа к удаленным данным, а рабочие места, на которых происходит анализ информации с использованием графики, — в режиме модели сервера управления данными.

1.3. Виды информационных ресурсов, хранимых и обрабатываемых в системе

В ИС предприятия хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации [17]. К *информации ограниченного доступа*, циркулирующей в МСС, относятся:

– персональные данные сотрудников предприятия и партнеров, хранимые в БД и передаваемые по сети;

– сообщения электронной почты и информация БД, содержащие служебные сведения, информацию о деятельности предприятия 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 предприятия;

– финансовая документация, бухгалтерская отчетность, аналитические материалы исследований о конкурентах и эффективности работы на финансовых рынках;

– другие сведения, составляющие деловую информацию о внутренней деятельности предприятия.

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

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

Внутри ИС выделяются внутренние информационные потоки:

– передача файлов между файловыми серверами и пользовательскими рабочими станциями;

– 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» и др.

В качестве внешних информационных потоковвыделяются:

– передача отчетных документов (производственные данные) от филиалов предприятия, по каналам корпоративной сети, а также с использованием отчуждаемых носителей;

– передача финансовых и статистических отчетных документов от филиалов предприятия;

– внутриведомственный и межведомственный обмен электронной почтой.

– различные виды информационных обменов между ИС и сетью Интернет, в том числе с использованием сетей мобильной связи.

1.4. Определение основных приоритетов информационной безопасности ИС

1.4.1. Базовые услуги безопасности

Стандарт [6] определяет пять базовых услуг для обеспечения безопасности (защиты) компьютерных систем и сетей, входящие в архитектуру защиты ЭМ: конфиденциальность (Confidentiality), аутентификацию (Authentication), целостность (Integrity), контроль доступа (Access Control), причастность Nonrepudiation). Стандарт определяет и механизмы, обеспечивающие функционирование этих услуг для обеспечения безопасности на уровнях коммуникации (с установлением соединения и без него), пакетов или отдельных полей. Этот набор услуг не является единственно возможным, однако он является общепринятым. Ниже описаны услуги и варианты их реализации, а также их отношения между собой и к модели взаимодействия открытых систем (ВОС).

Конфиденциальность. В указанном стандарте конфиденциальность определена как «свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных (неуполномоченных) личностей, объектов или процессов». Для этой услуги определяется четыре версии: для систем с установлением связи; для систем без установления связи; защита отдельных информационных полей; защита от контроля трафика.

Аутентификация. В указанном стандарте определяются два типа услуг аутентификации: достоверность происхождения (источника) данных и достоверность собственно источника соединения или объекта коммуникации (*peer-entity*).

Целостность. Согласно стандарту, 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.

Контроль доступа. Согласно стандарту, контроль доступа определен как «предотвращение неавторизованного использования ресурсов, включая предотвращение использования ресурсов недопустимым способом», т. е. данная услуга не только обеспечивает доступ авторизованных пользователей (и процессов), но и гарантирует указанные права доступа для авторизованных пользователей. Таким образом, эта услуга предотвращает неавторизованный доступ как «внутренних», так и «внешних» пользователей.

Контроль доступа часто ассоциируется с аутентификацией и конфиденциальностью, но на самом деле эта услуга предоставляет более широкие возможности, например, для установления политики контроля/ограничения доступа. Политика контроля доступа (или авторизации) 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 являются объектом контроля доступа на прикладном, 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.

Причастность («неотпирательство»). В стандарте причастность определяется, как «предотвращение возможности отказа одним из реальных корреспондентов коммуникаций от факта его полного или частичного участия в передаче данных». Определены две формы причастности: причастность к посылке сообщения и подтверждение (доказательство) получения сообщения. 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.

Доступность. Доступность может быть определена как дополнительная услуга обеспечения защищенности сетей и стать поводом для 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.

1.4.2. Реализация базовых услуг безопасности и анализ их применения

Для реализации базовых услуг безопасности в сети (см. табл. 1.1) 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 [6]. При этом практическая реализация требований ПОЛИТИКА может потребовать различных сочетаний базовых услуг защиты в соответствии с их приоритетами с учетом дифференциации по классу трафика. В табл. 1.1. приведена возможная реализация услуг безопасности отдельными специальными механизмами защиты или их сочетанием. 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. На практике услуги безопасности должны быть включены в соответствующие уровни логической структуры архитектуры сети для обеспечения требований защиты корпоративной сети.

Талица 1.1

Реализация базовых услуг безопасности

	Используемые специальные механизмы защиты							
Услуги безопасности	Шифрование	Заполнение трафика	Управление маршрутизацией	Цифровая подпись	Контроль доступа	Обеспечение целостности	Аутентификация	Нотаризация (подтверждение)
Конфиденциальность: - с установлением связи	–	+	+	–	–	–	–	–
- без установления связи	+	+	+	–	–	–	–	–
- отдельных информационных полей	–	–	–	–	–	–	–	–
- трафик	–	+	–	–	–	–	–	–
Аутентификация: - отправителя данных	+	–	–	+	–	+	+	–
- равноправного логического объекта	+	–	–	+	–	+	+	–
Целостность: - с установлением связи	–	–	+	–	–	+	–	–
- без установления связи	+	–	+	–	–	+	–	–
- отдельных информационных полей	+	–	–	–	–	+	–	–
Контроль доступа	–	–	–	–		–	–	–
Причастность: - отправка и доставка	–	–	–	+		–	–	+
Доступность	–	–	+	–		–	+	–

Сравнение базовых моделей архитектур OSI и DARPA–QoS приведено на рис. 1.6.

№ п/п	Модель OSI		№ п/п	Модель архитектуры DARPA -QoS
7	Прикладной A			Верхний H
6	Представлений P			
5	Сессий S			
4	Транспортный T		4	Транспортный T
3	Сетевой N		3	Межсетевой IP
2	Канальный L		2	Сетевого интерфейса (доступа), NA
1	Физический Ph		1	Физический,Ph

Рис.1.6. Модели архитектур OSI и DARPA-QoS

Применимость сервисов безопасности на различных уровнях модели ВОС приведена в табл.1.2. В ячейках, 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.

Таблица 1.2

Применимость сервисов безопасности

Услуга безопасности	Уровни в модели DARPA				
	1	2	3	4	5
Конфиденциальность: - с установлением связи	+	+	+	+	+
- без установления связи	–	+	+	+	+
- отдельных информационных полей	–	–	+	–	+
- трафик	+		+	–	+
Аутентификация: - отправителя данных	–	?	+	+	+
- равноправного логического объекта	–	–	+	–	–
Целостность: - с установлением связи	–	–	+	+	+
- без установления связи	–	?	+	+	+
- отдельных информационных полей	–	–	–	–	+
Контроль доступа	–	?	+	+	+
Причастность: - отправка и доставка	–	–	–	–	+

Организация защищенного сеанса связи с установлением соединения предусматривает запрос/подтверждение услуг безопасности на фазе установления защищенного соединения. Если служба безопасности

выступает 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 [19].

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) [6,20].

Услуга безопасности – это функциональные возможности h–уровня, которые предоставляются в распоряжение (h+1)–объектам в h–точках доступа к сервисам (СТД) h-уровня, которые играют роль логических интерфейсов (правил взаимодействия между смежными уровнями) между h-объектами и (h+1)-объектами двух смежных уровней.

Точка доступа к сервису–это точка, через которую запрашивается и предоставляется сервис уровня. Каждая точка доступа к сервису имеет индивидуальный адрес, который однозначно идентифицирует конкретный объект (h+1) –уровня, использующий сервис h–уровня, т.е. местоположение h–СТД определяется h–адресом (рис. 1.7). Между (h+1) –объектами, h–объектами и h–СТД существуют определенные соотношения. Во-первых, объекты, имеющие общую СТД, находятся в одной системе. Во-вторых, (h+1) –объект может быть подключен к нескольким h–СТД, соединенным с одними и теми же несколькими h–объектами. Однако в каждый момент каждая N–СТД соединена только с одним N–объектом и только с одним (h+1)–объектом, т. к. h–СТД является «входом» в определенный h– и (h+1)–объект и связана поэтому с идентификацией (адресацией) объектов.

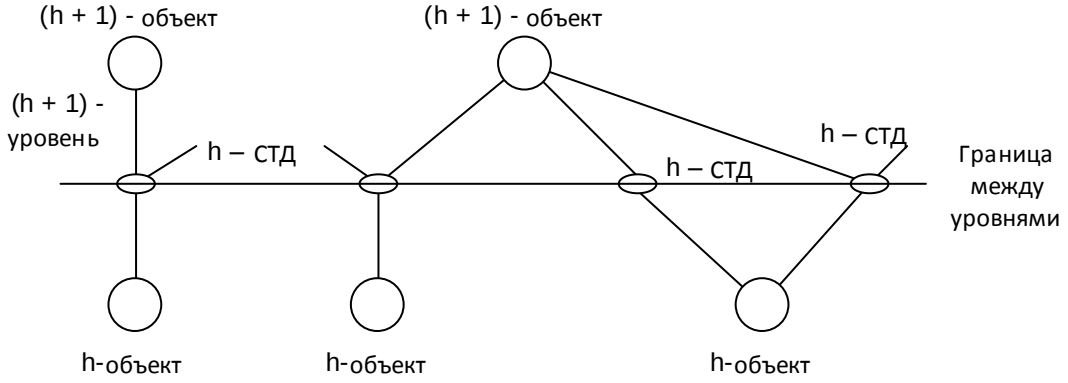

Рис.1.7. Схема предоставления услуги безопасности h–уровня в h–СТД

Одноранговые объекты h–уровня взаимодействуют между собой с помощью одного или нескольких протоколов через логические соединения, создаваемые на (h–1)–уровне. Спецификация протоколов h–уровня определяет процедуры выполнения сервисов, форматы управляющих и информационных полей протокольных блоков уровня (сервисных

примитивов уровня), процедуры обмена протокольными блоками между объектами h–уровня в разных открытых системах, а также механизм выбора указанных процедур из списка возможных. Сервисные примитивы – это концептуальные понятия, облегчающие описание последовательности событий при доступе к сервису уровня и представляют первичные, неделимые элементы описания сервиса. Каждый сервисный примитив является именованной (т. е. имеющей уникальное название) совокупностью параметров. Концепция сервиса, предоставляемого уровнем, является одной из основных в модели ВОС.

Сервис уровня определяется через элементы абстрактной модели взаимодействия пользователей сервиса и поставщика сервиса. Эта модель включает в себя следующие понятия (рис.1.8): пользователи N–сервиса, поставщик N–сервиса и сервисные примитивы. Последние разделяются на примитивы: запроса (request), индикации (indication), ответа (response) и подтверждения (confirmation).

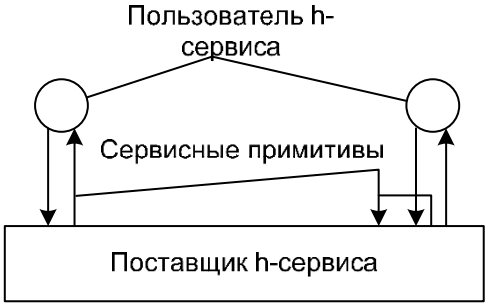

Рис.1.8. Модели взаимодействия пользователей сервиса и поставщика сервиса

Услуги безопасности представляют собой абстрактные понятия, которые характеризуют требования безопасности и могут быть реализованы на одном и/или нескольких логических уровнях архитектуры сети. Услуги безопасности могут быть обязательными и факультативными, а также подтвержденными и неподтвержденными. Обязательность услуги означает, что она должна предоставляться во всех реализациях. Факультативные услуги могут предоставляться или нет в зависимости от назначения реализации. Если сервис безопасности определяется в качестве факультативно предусматриваемой отдельным уровнем, это означает, что он 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. Подтверждаемые услуги – это те, предоставление которых связано с обменом парой сервисных примитивов – примитивом запроса и примитивом подтверждения. Для некоторых неподтверждаемых услуг обмен сервисными примитивами отсутствует – здесь достаточно только передачи запроса от

пользователя сервиса. Изложенные понятия являются основой формализованного описания сервиса. Элементы такого описания в настоящее время стандартизованы МОС и называются соглашениями по сервису.

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:

– идентификация равноправных объектов (в интервалах);

– защита выбранных полей;

– 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.

Задействование механизмов защиты может быть реализовано как в виде отдельных процедур, так и являться неотъемлемой частью протоколов установления соединения. Механизмы защиты, предоставляющие 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 возможно – фазы формирования и передачи сервисных примитивов трафика безопасности на дополнительном логическом уровне архитектуры сети и фазу их обработки в конечных и/или промежуточных системах с учетом QoS–норм передачи основных информационных потоков (*Приложение 1*). В любом случае реализация механизмов защиты осуществляется по принципам предоставления сервиса ВОС [19].

1.5. Определение приоритетов применения базовых услуг безопасности в ИС

Политика информационной безопасности ИС в зависимости от ее назначения может строится в соответствии с различными приоритетами реализации базовых услуг безопасности в порядке убывания их важности [17].

Для «закрытого» контура приоритеты базовых услуг безопасности определяются следующей иерархией:

– конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации;

– целостность хранимой, обрабатываемой и передаваемой по каналам связи информации;

– доступность информации (обеспечение устойчивого функционирования системы).

Для «открытого» контура приоритеты определяются следующей иерархией:

– целостность хранимой, обрабатываемой и передаваемой по каналам связи информации;

– доступность информации;

– конфиденциальность передаваемой по открытым каналам связи информации.

Контрольные вопросы по гл. 1

1. На основе какого документа определяется информационная безопасность организации?
2. Какие этапы включает процесс построения политики информационной безопасности ИС организации?
3. Какие функциональные элементы входят в состав типовой ИС организации (объекта защиты)?
4. Какие основные преимущества и недостатки различных архитектур «клиент-сервер»?
5. Какие виды информационных ресурсов могут передаваться, храниться и обрабатываться в ИС?
6. Какие услуги безопасности относятся к базовым услугам безопасности согласно ГОСТ Р ИСО 7498-2–99?
7. Какие механизмы безопасности относятся к специальным и общим?
8. Как организовано уровневое применение базовых услуг безопасности в эталонной модели ВОС.
9. Что определяет запрос, формируемый логическим объектом (h+1), к услуге защиты h–уровня?
10. Какая иерархия основных приоритетов базовых услуг безопасности в «закрытом» и «открытом» контурах ИС?

Глава 2. Модели нарушителя и угроз в информационной системе

2.1. Модели нарушителя в ИС

2.1.1. Модель нарушителя в «закрытом» контуре

В «закрытом» контуре модель нарушителя и угроз строится с учетом обеспечения следующих приоритетов базовых услуг безопасности: *конфиденциальности, целостности и доступности активов «закрытого» контура* [15-17].

Под нарушителем понимается человек или группа лиц, имеющая своей целью нанесение ущерба пользователям ИС 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 процесс, выполняемый на вычислительных средствах «закрытого» контура. Все физические лица, имеющие доступ к ресурсам ИС, могут быть отнесены:

– к категории I - лица, не имеющие права доступа в контролируемую зону, в которой располагаются ресурсы ИС;

– к категории 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 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 [17]:

1.Внешний нарушитель (группа Н1), не являющийся пользователями «закрытого» контура, – субъект, имеющий доступ на контролируемую территорию ИС, но не имеющий доступа к работе со штатными средствами «закрытого» контура. К этой группе нарушителей относится администратор ЛВС «открытого» контура.

2.Внешний нарушитель (группа Н2), осуществляющий атаки с удаленных рабочих мест корпоративной сети, использует возможности доступа к информации, передаваемой по соответствующим протоколам информационного обмена, с целью внедрения в «закрытый» контур ИС;

3.Внутренний нарушитель, не являющийся пользователем «закрытого» контура ИС и не имеющий доступа к информации и работе со штатными средствами (группа 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, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС под контролем пользователей.

4.Внутренний нарушитель (группа Н4) 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.

5.Внутренний нарушитель (группа 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.

6.Внутренний нарушитель (группа 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) отвечающий за управление и конфигурирование СУБД, обеспечение непрерывного сервиса СУБД;

б) администратор БД (Н6б) занимающийся разграничением прав доступа к объектам БД, управляющий созданием, модификацией и удалением объектов;

в) администратор ОС (Н6в) занимающийся управлением и конфигурированием ОС. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы СУБД и клиентов системы, является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС;

г) администратор аппаратной платформы (АП) (Н6г) занимающийся управлением и конфигурированием аппаратной платформы.

д) администратор СИБ «закрытого» контура (Н6д) 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 необходимо также предусмотреть возможные несанкционированные действия разработчиков ИС на этапах ее разработки, внедрения и сопровождения.

*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.

Описание объектов и целей атак. К объектам атак (объектам защиты) «закрытого» контура относятся:

– информация, обрабатываемая, передаваемая и хранимая с использованием технических средств «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 (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 только по отношению к субъекту).

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.

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 (не декларированных) возможностей средств защиты, внесенных: а) в процессе разработки этих средств (Н1– Н6); б) при

транспортировке этих средств (Н1– Н6); в) при создании и наладке системы защиты (Н1, Н3 – Н6);

– атаки при считывании или восстановлении 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 – Н6);

– атаки при негласном (скрытом) временном изъятии съемных носителей защищаемой информации, аутентифицирующей или ключевой информации (Н3 – Н6);

– атаки при негласной (скрытой) модификации защищаемой информации, хранящейся на съемных носителях информации (Н4, Н5, Н6);

– при визуальном просмотре защищаемой информации на экране монитора (Н3 – Н6);

– при ознакомлении с распечатанной защищаемой информацией (Н3 – Н6);

– при выводе информации на неучтенные носители (в том числе, при выводе на печать), а также при нарушении требований руководящих и нормативных документов, регламентирующих порядок обращения с информацией соответствующей категории доступа (Н4–Н6);

– при доступе к оставленным без присмотра функционирующим штатным средствам «закрытого» контура ИС (Н3–Н6);

– при несанкционированном изменении конфигурации технических средств «закрытого» контура ИС (Н6г);

– при подборе 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);

– при вызывании сбоев технических средств «закрытого» контура ИС (Н3–Н6);

– при внесении неисправностей в технические средства «закрытого» контура ИС (Н3–Н6);

– при блокировании или уничтожении информации, технических, программных и программно-технических компонентов «закрытого» контура ИС (Н2–Н6);

– при несанкционированном доступе 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–Н6).

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

2.1.2. Модель нарушителя в «открытом» контуре

В «открытом» контуре модель нарушителя, как правило, строится с учетом обеспечения приоритетов базовых услуг безопасности – *целостность,доступность и конфиденциальность*. При разработке модели нарушителя предполагается, что [15-17]

– 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» 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 (группы Н2 и Н1) – субъекты, не имеющий доступа на контролируемую территорию объектов размещения ТС «открытого» контура ИС, - пользователи взаимодействующих ведомственных систем, а также пользователи сети Интернет.

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.

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.

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.

Предположения об имеющихся у нарушителя средствах атак. Нарушитель может использовать следующие средства атак:

– штатные средства «открытого» контура ИС;

– доступные в свободной продаже и 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, Н1);

– на каналы связи, выходящие за пределы контролируемой зоны объектов, на которых располагаются технические средства «открытого» контура ИС (нарушители Н2, Н1).

Возможности внешнего нарушителя (Н2, Н1) существенно зависят от степени защищенности используемых каналов связи (применение криптографических средств защиты, межсетевых экранов, средств обнаружения компьютерных атак и др.). Возможными направлениями действий внешнего нарушителя (Н2, Н1) 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 (Н1, Н2) может проводить атаку только из-за пределов контролируемой зоны. Нарушитель (Н1, Н2) 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.

2.2. 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 управления хозяйствующих субъектов ИС при внедрении, контроле (мониторинге эффективности) и совершенствовании системы обеспечения информационной безопасности (СОИБ). Требования ИБ разрабатываются на базе моделей нарушителя и угроз.

При построении СИБ ИС в первую очередь необходимо определить 1) какие угрозы должны быть устранены и в какой мере; 2) какие ресурсы ИС должны быть защищены и в какой степени; 3) с помощью каких механизмов должна быть реализована защита и какая стоимость ее реализации и затраты на эксплуатацию средств защиты.

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. 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. При этом *атаки определены, если определены объект, цель, канал и способ нападения, а также средства нападения*.

Предполагается, что защита от угроз, не являющихся атаками, в основном регламентируется инструкциями, разработанными и утвержденными подразделениями, эксплуатирующими ИС с учетом особенностей эксплуатации и действующей нормативной базы.

Угрозы информационной безопасности, с точки 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.

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. Как внешние, так и внутренние нарушители, и природные явления являются источниками угроз безопасности технических средств системы.

Отдельно следует рассмотреть угрозы безопасности корпоративной сети. 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:

– 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.).

Угрозы, реализуемые с использованием программных средств- 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, используя возможности, предоставляемые ПО ИС. Большинство рассматриваемых в этом классе угроз реализуется путем осуществления локальных или удаленных атак на информационные ресурсы системы внутренними и внешними злоумышленниками. 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 не декларированных возможностей, оставленных для отладки, либо умышленно внедренных;

– наблюдение за работой системы путем использования программных средств анализа сетевого трафика и утилит ОС;

– 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;

– ошибки ввода управляющей информации с АРМ операторов в БД;

– блокирование работы пользователей системы программными средствами и др.

Совокупность возможных угроз со стороны потенциального злоумышленника с учетом имеющихся в его распоряжении сил и средств на некотором интервале времени образуют *модель защиты ИС*. Модель защиты ИС — некоторая упорядоченная совокупность всей доступной информации о возможных угрозах и условиях их осуществления со стороны потенциального злоумышленника, наносимом ущербе, о защитных свойствах ИС и используемых в ней средствах защиты информации.

2.2.1. Модели угроз «закрытого» контура

Как было отмечено выше, для «закрытого» контура приоритеты базовых услуг безопасности, следующие]:

– *конфиденциальность* хранимой, обрабатываемой и передаваемой по каналам связи информации;

– *целостность* хранимой, обрабатываемой и передаваемой по каналам связи информации;

– *доступность* информации (обеспечение устойчивого функционирования системы).

Основные угрозы нарушения *конфиденциальности* в «закрытом» контуре [16, 17].

*Для серверов ИС (ОС и СУБД)**:***

– ознакомление с конфиденциальными данными лиц, не допущенных к этой информации;

– создание незарегистрированных незаконных копий информационных массивов;

– кража носителей (оптические диски, USB-устройства и цельные ПК), производственные отходы (распечатки, записи, списанные носители и т.д.).

*Для корпоративной сети**:***

– перехват административных паролей серверов и сетевого оборудования с помощью прослушивания сети (сниффинга);

– перехват конфиденциального трафика путем прослушивания;

– захват IP-соединений и полномочий администратора или пользователя (технологии спуффинга);

– перехват передаваемых данных с целью их хищения, модификации, разрушения или переадресации;

– несанкционированная отправка данных от имени другого пользователя;

– несанкционированное использование сетевых ресурсов;

– отрицание пользователями подлинности данных, а также фактов отправления или получения информации;

– формирование ложных ICMP-пакетов для изменения параметров маршрутизации;

– использование слабых мест в сетевых службах для разрушения сетевых ресурсов;

– использование слабых мест системы DNS для создания ложных таблиц хостов;

– использование слабых мест почтовой системы для проникновения в почтовую машину;

– использование протокола SNMP управления сетью для получения сведений о сетевом оборудовании и возможного перехвата и замены управляющих сообщений;

– подбор паролей;

– занесение вируса с почтовой корреспонденцией.

Для систем защиты от НСД и средств криптографической защиты информации:

– компрометация ключевой информации;

– расшифровка криптографически защищенной информации с использованием методов криптоанализа.

Поразив конфиденциальность компонент «закрытого» контура (например, перехватив административные пароли) нарушитель может исказить какой-либо конфигурационный файл и тем самым осуществить атаку на целостность и доступность системы.

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

Для серверов ИС (ОС и СУБД):

– несанкционированное изменение базы данных ИС;

– несанкционированное изменение компонентов ОС и СУБД;

– несанкционированное изменение программного обеспечения ИС;

– несанкционированное изменение операционной среды АРМ.

Для АРМ:

– несанкционированное изменение операционной среды АРМ;

– действия нарушителя в среде ИС от имени законного пользователя, которые являются деструктивными или приводят к искажению информации.

Для ОС ЛВС:

– несанкционированноеизменение конфигурации и режимов работы файлового сервера ЛВС.

Для корпоративной сети:

– внесение несанкционированных изменений в настройки аппаратуры связи.

Нарушитель, поразив целостность компонент «закрытого» контура, может заблокировать его нормальное функционирование и таким образом атаковать доступность системы.

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

*Для северов ИС (ОС и СУБД)**:***

– дистанционные атаки на сетевые службы с целью нарушения их работы (перехват паролей и трафика, атаки типа "отказ в обслуживании", использование уязвимостей услуг);

– локальные атаки на систему защиты ОС со стороны законного пользователя (выбор пароля, использование уязвимостей файловой системы, настроек сервиса и драйверов) с целью нарушения работы серверов ИС;

– неквалифицированные или незаконные действия администраторов ОС и СУБД, приводящие к нарушению работы ИС.

Для автоматизированного рабочего места:

– несанкционированное изменение конфигурации ОС (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС Windows);

– несанкционированное удаление (модификация) исполняемых файлов прикладного и системного программного обеспечения;

– внесения компьютерных вирусов;

– несанкционированная работа программ, выполняющих некорректные действия из-за ошибок или специальных закладок.

Особенно это касается специализированных сложных вредоносных программ (например, таких вирусов, как Stuxnet и Flame), направленных на решение специальных задач по компрометации конкретных систем и ресурсов разведывательными, деструктивными, диверсионными и другими целями [21]. Направленные воздействия на ИС, которые могут быть выполнены внутренним легальным нарушителем через USB-интерфейс вычислительных средств с целью нарушения их функционирования. Они могут осуществляться через следующие элементы:

– сетевые и коммуникационные каналы;

– порт тестового доступа микросхем (Test Access Port - TAP). Широко распространенным стандартным портом тестирования является порт сканирования границ Boundary Scan (JTAG) IEEE 1149.1-2001 и IEEE 1149.6-2003 порт;

– ПЗУ начальной загрузки (обновлении программы BIOS);

– периферийные интерфейсы, такие как SATA, USB и др.;

Реализация аппаратных «закладок» также не исключена на этапе изготовления микросхем, модулей и ЭВМ, исполнительные механизмы которых могут иметь различные целевые направления для потенциального повреждения функций ИС, включая его полную блокировку.

Минимизировать остаточные риски наличия вредоносного кода в компонентах ИС «закрытого» контура, особенно в ИС специального назначения, обеспечивается проведением сертификационных испытаний

(тематических исследований) в различных государственных системах сертификации, например, ФСТЭК России и др.

Для ОС ЛВС:

– дистанционные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа "Отказ в обслуживании", использование уязвимостей сервиса);

– внесение изменений в ПО, хранящееся на серверах LAN, что приводит к нарушению работы пользователя.

Для корпоративной сети:

– отказ или несанкционированное изменение конфигурации сетевого оборудования, приводящее к потере доступа к сетевым ресурсам, что может проявляться как в сбое обслуживания, так и в изменении алгоритмов управления (перехват управления).

Для систем защиты от НСД и средств криптографической защиты информации:

– дистанционные 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.

Нарушение доступности информационных, программных и аппаратных ресурсов может привести к нарушению процесса обработки информации (несанкционированное отключение СУБД, ОС, уничтожение данных и т.д.).

Реализация цифровой экономики в нашей стране связана с внедрением новых инфокоммуникаций, одним из элементов которых является третья платформа информатизации (ТПИ) [22]. Эта платформа объединяет:

– облачные вычисления, безопасность которых связана с виртуализацией логически разделяемых вычислительных процессов и физических вычислительных ресурсов;

– интернет вещей, ставший частью киберпространства, безопасность которого связана с соединением физических вещей с цифровыми датчиками, с интеграцией аналогового мира и его цифровым описанием, что делает необходимым обеспечение информационно-энергетической, информационно-транспортной, информационно-производственной и в целом информационно-экономической безопасности;

– большие данные, безопасность которых связана с возможностью путем их обработки, в том числе и с деструктивными целями, делать достаточно точные статистические оценки о состоянии дел во всех областях деятельности государств, а также силовых министерств и ведомств РФ;

– мобильный широкополосный доступ, безопасность которого связана с отсутствием границы сети, на которой можно было бы блокировать атаки;

– наложенные сервисы, безопасность которых связана, помимо традиционных угроз (Web-атаки, фишинг и т. д.), с появлением рисков и

угроз при олицетворении пользователей в социальной сети и необходимо учитывать, что процессы и темы общения в социальных сетях могут быть целенаправленно организованы противником с помощью инструментов социальной инженерии.

Необходимо отметить, что внедрение ТПИ одновременно с предоставлением новых инфокоммуникационных услуг создает и угрозы нового типа, связанные со средой виртуализации [1, 22] (табл.2.1).

Таблица 2.1.

Услуги ТТИ и значимые угрозы нового типа

Услуги третьей платформы информатизации	Угрозы нового типа
Облачные вычисления	Угрозы, связанные с виртуализацией логически разделяемых вычислительных процессов и физических вычислительных ресурсов
Интернет-вещи	Угрозы, связанные с соединением физических вещей с цифровыми сенсорами, с объединением аналогового мира и его цифрового описания
Большие данные	Угрозы, связанные с обработкой больших данных в деструктивных целях
Мобильный широкополосный доступ	Угрозы, связанные с отсутствием границы сети, на которой можно было бы блокировать атаки
Наложенные сервисы	Угрозы, связанные с обезличиванием пользователей в социальной сети

Анализ угроз, приведенных в табл.2.1. и угроз, приведенных в новой доктрине ИБ Российской Федерации [1] показывает, что эффективность защиты информационных интересов РФ напрямую зависит от внедрения технологий ТПИ.

2.2.2. Модели угроз в «открытом» контуре

Для «открытого» контура определяются следующие приоритеты:

– *целостность* хранимой, обрабатываемой и передаваемой по каналам связи информации;

– *доступность* информации (при необходимости);

– *конфиденциальность* передаваемой по открытым каналам связи информации (при необходимости).

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.

Одним из способов идентификации угроз является построение модели нарушителя [17].

Контрольные вопросы по гл. 2

1. Какие работы проводятся в процессе анализа рисков?
2. Как осуществляется идентификация и определение ценности всех активов ИС?
3. Как осуществляется идентификация угроз и уязвимостей для ценных активов?
4. В чем заключается оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении ценных активов;
5. Какие существуют критерии принятия рисков?
6. Какие два основных метода известны оценки рисков безопасности ИС?
7. Какие этапы включает алгоритм обработки рисков ИС реализующего метод, основанный на модели угроз и уязвимостей?
8. Какие этапы включает алгоритм обработки рисков ИС реализующего метод, основанный на модели информационных потоков?
7. Как строится модель нарушителя в ИС «закрытом» контуре ИС?
8. Как строится модель нарушителя в ИС «открытом» контуре ИС.
9. Какие значимые угрозы в ИС «закрытого» контура?
10. Как строится модель угроз в ИС «закрытого» контура?
11. Какие значимые угрозы в ИС «открытого» контура?
12. Как строится модель угроз в ИС «открытого» контура?

Глава 3. Требования к построению защищенной информационной системы

3.1.Общие требования к подсистемам«закрытого» и «открытого» контуров ИС

При построении системы ИБ «закрытого» и «открытого» контура ИС организации в ней должны быть реализованы следующие общие подсистемы:

– резервирования и восстановления информации;
– контроля эталонного состояния информации и рабочей среды;
– управления безопасностью;
– антивирусной защиты информации;

3.1.1. Общие требования к подсистеме резервирования и восстановления информации

Подсистема резервного копирования и восстановления предназначена для обеспечения непрерывной работы ИС и ее восстановления путем резервного копирования программ и данных и их восстановления из резервных копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение её задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т. д. Рабочие конфигурации серверов, на которых хранится и обрабатывается конфиденциальная информация, подлежат резервному копированию.

Все программное обеспечение, используемое в системе, должно иметь справочные (дистрибутивные) копии. Их местоположение и информация об ответственных за их создание, хранение и использование должны быть указаны в формах для каждого АРМ. Также указываются перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственных за создание, хранение и использование страховых копий данных.

Соответствие состояния защищаемых информационных ресурсов и рабочих конфигураций серверов и АРМ, обрабатывающих конфиденциальную информацию, контролируется подсистемой управления эталонным состоянием информации и рабочей средой.

Быстрое восстановление программ с использованием справочных копий и данных, включенных в перечень неизменяемых защищенных информационных ресурсов (с использованием страховых копий) в случае уничтожения или повреждения в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (в отношении основных компонентов системы) хранением копий.

3.1.2. Общие требования к подсистеме контроля эталонного состояния информации и рабочей среды

Подсистема контроля эталонного состояния информации и рабочей среды предназначена для фиксации и динамического контроля изменений состояния наборов данных, эталонного состояния параметров рабочей среды путем сравнения текущих характеристик контролируемых объектов с эталонными характеристиками.

Должна быть предусмотрена возможность выбора объектов ИС для проверки их соответствия стандарту. Объекты выбираются на основе перечня защищаемых информационных ресурсов и частоты их изменений, а также перечня программных средств, участвующих в обработке конфиденциальной информации и степени их влияния на работу защищаемых ИС.

Контрольное состояние должно контролироваться динамически, в соответствии с нормативами, при загрузке ОС серверов, рабочих станций, при регистрации пользователей в ИС или в системе безопасности. Должна быть реализована функция периодической проверки.

Результаты проверок должны быть отправлены в подсистему управления безопасностью для обработки.

3.1.3. Общие требования к подсистеме управления безопасностью

Подсистема управления безопасностью предназначена для контроля эффективности защиты, регистрации данных о событиях в ИЭ, событиях в системе безопасности, автоматизированной обработки данных и поддержки принятия решений о разработке управляющих действий на других подсистемах системы безопасности посредством сбора и автоматизированной обработки регистрационных данных.

Подсистема управления безопасностью должна выполнять функции обновления системы безопасности. Комплексный подход к обеспечению актуальности системы информационной безопасности должен охватывать следующие функциональные области:

– периодический и, по возможности, динамический контроль безопасности, обеспечивающий своевременное обнаружение возникающих уязвимостей, которые могут быть использованы для проведения атак;

– обнаружение атак в режиме реального времени, что позволяет своевременно выявлять и локализовать попытки совершения несанкционированных действий и выявлять факты несанкционированного воздействия на компьютерные ресурсы;

– централизованное и упреждающее управление, обеспечивающее автоматизированную поддержку принятия решений, а также эффективный контроль за пользователями и ресурсами сети для уменьшения количества ошибок администрирования и принятия упреждающих мер для предотвращения наихудших событий.

Контроль защищенности должен обеспечивать периодическое, а в некоторых случаях динамическое, выполнение следующих базовых функций:

– проверка системы безопасности на соответствие новым руководящим принципам и нормативным документам в области информационной и компьютерной безопасности;

– контроль за правилами правильного использования средств защиты в зависимости от их состава и назначения;

– контроль целостности и подлинности компонентов системы безопасности;

– контроль правильного изменения параметров конфигурации системы безопасности;

динамическая регистрация данных о функционировании системы защиты, их анализ и уведомление ответственных лиц в случае нарушения правильности средств защиты;

– тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак;

– контроль работоспособности подсистем защиты при имитации неисправностей отдельных элементов компьютерной сети;

– проверка на отсутствие ошибок администрирования и конфигурации;

– анализ политики формирования и использования справочной информации (ключей, паролей и т.д.);

– проверка на своевременность обновления программного обеспечения;

– проверка на отсутствие программных закладок и вирусов.

Проверка системы безопасности на соответствие соответствующим руководящим принципам и правилам в области информационной и компьютерной безопасности должна обеспечивать своевременное выявление недостатков в системе безопасности на основе анализа передовой практики систематизации требований к таким системам.

Контроль за соблюдением правил правильного использования средств защиты в зависимости от их состава и назначения заключается в периодическом контроле и пересмотре политики в области безопасности на ее административном и процедурном уровнях. При изменении структуры, шаблонов процессов или условий работы компьютерной системы концепция безопасности и подробные процедурные меры могут изменяться, в частности, конкретная информация и инструкции по компьютерной безопасности, относящиеся к администраторам и пользователям компьютерной системы. Контроль целостности и подлинности компонентов системы защиты предполагает периодический или динамический контроль:

– наличия требуемых резидентных компонентов системы защиты в оперативной памяти компьютера;

– всех программ системы защиты, находящихся во внешней и оперативной памяти, на соответствие эталонным характеристикам;

– корректности параметров настройки системы защиты, располагаемых как в оперативной, так и во внешней памяти;

– корректности эталонной информации (идентификаторов, паролей, ключей шифрования и т.д.).

При проверке правильности изменения параметров конфигурации системы безопасности подсистема мониторинга не должна разрешать установку параметров, противоречащих политике безопасности, принятой в организации.

Запись данных о работе системы безопасности предполагает запись и накопление информации о последующих действиях всех подсистем безопасности, всех администраторов и пользователей других категорий по использованию средств безопасности.

Помимо регистрации данных о работе системы безопасности, следует обеспечить периодический анализ накопленной информации. Основной целью такого анализа является своевременное выявление недопустимых действий, а также прогнозирование степени защищенности информации и её обработки в компьютерной системе.

Для проведения периодического анализа необходимо заранее подготовить правила описания политики функционирования системы защиты по одному из принципов: «допустимо все, что не запрещено в работе системы защиты» и «запрещено все, что явно недопустимо».

Более высокий уровень контроля и безопасности обеспечивается вторым принципом, так как на практике не всегда можно в полной мере учитывать все действия, которые запрещены. Надежнее выявить все разрешенные действия и запретить все остальные.

Если подсистема мониторинга обнаруживает какие-либо нарушения в надлежащем функционировании подсистемы безопасности, соответствующие представители безопасности должны быть немедленно уведомлены.

Тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак осуществляется с помощью специализированных средств анализа безопасности, которые, как правило, обеспечивают выполнение оставшихся функций контроля безопасности.

3.1.4. Подсистема антивирусного контроля

Подсистема антивирусного контроля должна реализовать архитектуру, позволяющую организовать централизованное управление антивирусными шлюзами с помощью средств управления ИС, включающих антивирусную защиту рабочих станций и серверов как «закрытого», так и «открытого» контуров.

Архитектура антивирусных шлюзов должна основываться на принципе централизованного управления шлюзами как компонентами системы антивирусной защиты ИС. Антивирусные шлюзы должны быть реализованы в виде программных агентов, установленных на серверной ОС, используемой для взаимодействия в ИС, что должно обеспечить выполнение функций антивирусной проверки содержания информации, передаваемой по сетевым каналам.

Управление агентами должно осуществляться по защищенному логическому каналу с аутентификацией пользователя (защита должна обеспечиваться от наложения контрольных действий на агенты антивирусной системы).

Подсистема управления должна обеспечивать возможность создания логической структуры системы антивирусной защиты независимо от логической структуры ЛВС. Возможность включения в сегмент, защищенный антивирусными агентами, не должна зависеть от количества сетевых доменов, должна быть реализована сегментация сети посредством физической и логической сегментации, а также возможность управления агентами через брандмауэры. Агенты должны интегрироваться в системы передачи данных IS в качестве дополнительного модуля.

Во время работы подсистема антивирусного контроля должна обеспечивать:

– централизованный контроль антивирусной защиты в соответствии с правилами антивирусной защиты со стороны подразделения безопасности (администраторов антивирусной защиты) и передача данных, генерируемых в результате антивирусной проверки, в подсистему управления безопасностью;

– автоматический запуск при инициализации ИС, а также в ручном режиме. В активном режиме антивирусный контроль должен обеспечивать обнаружение вирусов в программах и файлах данных, получаемых по каналам связи и с отчуждаемых носителей. В пассивном режиме – запускаться как самостоятельная задача и после окончания текущей проверки завершать работу. Работать в пассивном режиме (как самостоятельная задача) и после окончания текущей проверки завершать работу.

3.2. Требования к подсистемам обеспечения ИБ «закрытого» контура

Подсистемы обеспечения безопасности «закрытого» контура типовой ИС организации должны обеспечивать:

– защиту информации от НСД;
– криптографическую защиту информации;
– контроль целостности;
– защиту межсетевого взаимодействия;
– администрирование;
– обнаружение и противодействие вторжений;
– резервирования и восстановления информации;
– контроля эталонного состояния информации и рабочей среды;
– управления безопасностью;
– мониторинг состоянии ИБ.

Основные требования к подсистемам «закрытого» контура приведены в [17].

3.2.1. Типовые требования к подсистеме защиты информации от НСД

Отметим, что при создании конкретной ИС Заказчик формирует требования по защите информации в том числе и в соответствии с классификацией защищенности ИС и средств вычислительной техники (СВТ) определяемой, в частности, Руководящими документами ФСТЭК [11-13] и др. Руководящим документом [11] устанавливается девять классов защищенности АС от НСД к информации. Необходимыми исходными данными для проведения классификации конкретной АС являются:

– перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

– перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

– матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

– режим обработки данных в АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

– наличие в АС информации различного уровня конфиденциальности;

– уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

– режим обработки данных в АС - коллективный или индивидуальный.

Руководящий документ [12] устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый.

Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных приведены в [14, 23].

При этом, Постановление Правительства РФ [23] устанавливает 4 уровня защищенности персональных данных, которые определяются видом ИСПДн, типом актуальных угроз и количеством субъектов ПДн, обрабатываемых в информационной системе (табл. 1).

Таблица 1

Классификация ИСПДн по уровням защищенности и типам угроз

Виды ИСПДн	Уровни защищенности ИСПДн		
	угрозы 1 типа	угрозы 2 типа	угрозы 3 типа
ИСПДн-С	1	2 < 100000 > 1	3 < 100000 > 2
ИСПДн-Б	1	Тип ИСПДн	3
ИСПДн-О	2	3 < 100000 > 2	4
ИСПДн-И	1	3 < 100000 > 2	4 < 100000 > 3

Виды ИСПДн категорируются по типам обрабатываемой информации.

ИСПДн-С – ИС персональных данных, обрабатывающая специальные категории ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни субъектов;

ИСПДн-Б – ИС персональных данных, обрабатывающая биометрические сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

ИСПДн-О – ИС персональных данных, обрабатывающая общедоступные ПДн;

ИСПДн-И – ИС персональных данных, обрабатывающая иные категории.

Подсистема защиты от НСД «закрытого» контура предназначена для разграничения доступа к сетевым, информационным и вычислительным ресурсам контура как со стороны пользователей и администраторов внутри контура, так и со стороны пользователей и администраторов «открытого» контура. Подсистема должна требовать от пользователей идентификации в запросах на доступ и аутентификации идентификатора - его аутентификации, а также. Запретить доступ к защищенным ресурсам неустановленных пользователей и пользователей, чье удостоверение не было аутентифицировано.

Механизмы управления доступом. Механизмы управления доступом используются для предоставления услуг управления доступом. Механизмы контроля доступа - это те, которые используются для усиления стратегии ограничения доступа к ресурсу через доступ только к тем субъектам, которые имеют на это полномочия. Управление доступом используется для определения полномочий отправителя данных устанавливать сеанс связи и/или использовать ресурсы в сеансе связи.

Требования, подходы и проблемы контроля доступа. Механизмы контроля доступа являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищенным информационно-техническим ресурсам - объектам. В качестве субъектов в простейшем случае понимается пользователь.

На практике механизмы управления доступом необходимы, даже если в системе может присутствовать только один пользователь приложения. Это связано с тем, что, как правило, в системе должна быть создана учетная запись пользователя с правами администратора, которая настраивает параметры системы безопасности и права доступа к ресурсам защищаемого объекта. При этом администратор имеет принципиально иные права, чем пользователь приложения.

Механизм контроля доступа реализует на практике некую абстрактную (или формальную) модель, определяющую правила установления политики

делимитации доступа к защищаемым ресурсам и правила обработки запросов на доступ к защищаемым ресурсам.

Дискреционная (матричная) модель. Рассмотрим так называемую матричную модель защиты (ещё называемую дискреционной моделью), ставшую более распространённой на практике сегодня. С точки зрения матричной модели система защиты описывается как S, O, M: где S - совокупность субъектов, являющихся активными структурными элементами модели; O - объекты множественного доступа, являющиеся пассивными защищёнными элементами модели. Каждый объект уникально заражен именем объекта; M - матрица доступа. Значение элемента матрицы M [S, O] обеспечивает права доступа субъекта S к объекту O.

Права доступа регулируют доступ субъекта S к различным типам объектов доступа. В частности, права доступа субъектов к файловым объектам обычно определяются как чтение (R), запись (W) и выполнение (E).

Основой реализации управления доступом является анализ строки матрицы доступа при обращении субъекта к объекту. При этом проверяется строка матрицы, соответствующая объекту, и анализируется, разрешены ли ей права доступа для субъекта или нет. На основании этого принимается решение о предоставлении доступа.

При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, матричным моделям присущи серьезные недостатки. Основной из них — это излишне детализированный уровень описания отношений субъектов и объектов. Из-за этого усложняется процедура администрирования системы защиты. Причем это происходит как при задании настроек, так и при поддержании их в актуальном состоянии при включении в схему разграничения доступа новых субъектов и объектов. Как следствие, усложнение администрирования может приводить к возникновению ошибок.

Многоуровневые (обязательные) модели. Для устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечного состояния Белла и ЛаПадулы, а также модель решетки Д. Демнинга. Многоуровневые модели предполагают формализацию процедуры присвоения прав доступа с помощью так называемых меток конфиденциальности или мандатов, назначенных субъектам и объектам доступа.

Таким образом, для объекта доступа, например, метки могут быть определены в соответствии с уровнем доступа человека к информации, а для объекта доступа (самих данных) признаки конфиденциальности информации. Признаки конфиденциальности ИС регистрируются в метке объекта.

В связи с использованием терминов «мандат», «метка», «полномочия» многоуровневую защиту часто называют соответственно либо мандатной защитой, либо защитой с метками конфиденциальности, либо полномочной защитой.

Права доступа каждого объекта и характеристики конфиденциальности каждого объекта отображаются как набор уровней конфиденциальности и набор категорий конфиденциальности. Уровень последовательности может принимать одну из строго упорядоченных серий для ИК предприятия фиксированных значений, например, конфиденциальных, секретных, для служебного пользования, необеспеченных и т. д. Основой реализации контроля доступа являются:

1. Официальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрашивался доступ.

2. Решения о предоставлении доступа основываются на определенных правилах, которые основаны на противодействии снижению конфиденциальности защищаемой информации.

Таким образом, многоуровневая модель предотвращает возможность преднамеренного или случайного снижения уровня конфиденциальности рассматриваемой информации из-за её утечки (умышленной передачи), то есть эта модель предотвращает передачу информации от объектов с высоким уровнем конфиденциальности и узким набором категорий доступа к объектам с более низким уровнем конфиденциальности и более широким набором категорий доступа.

Практика показывает, что многоуровневые модели защиты гораздо ближе к потребностям реальной жизни, чем матричные модели, и обеспечивают хорошую основу для построения автоматизированных систем разграничения доступа. Кроме того, поскольку отдельные категории одного уровня равны, для их различения наряду с многоуровневой (мандатной) моделью требуется применение матричной модели.

С помощью многоуровневых моделей можно значительно упростить задачи администрирования (настройки). Кроме того, это касается как первоначальной установки политики доступа с делителями (такой высокий уровень и детализация установки отношения «предмет-объект» не требуется), так и последующего включения новых субъектов и объектов доступа в схему администрирования.

Подсистема защиты от НСД «закрытого» контура должна обеспечивать:

– однозначную идентификацию пользователей в ИС и в операционной системе (далее – ОС) АРМ (использование общих идентификаторов (ни в СЗИ, ни в ОС) не допускается;

– идентификацию по логическим именам информационных ресурсов (логических устройств, каталогов, файлов);

– исключение возможности удаленного подключения к локальным ресурсам «закрытого» контура и управление доступом к этим ресурсам за счет настроек ОС и СЗИ АРМ «закрытого» контура;

– управление доступом между «закрытым» контуром и «открытым» контуром на основе применения технологии межсетевых экранов (далее – МЭ);

– мандатное (многоуровневое) разграничение доступа субъектов «закрытого» контура к объектам с помощью маркеров доступа СЗИ ОС доменных пользователей и меток конфиденциальности объектов, хранящихся в их дескрипторах безопасности таблиц контроля доступа (далее – ТРД). Мандатное разграничение доступа должно быть реализовано в соответствии с моделью Белла-ЛаПадула:

а) классификационные метки безопасности каждого субъекта и каждого объекта должны соответствовать, отражая их место в соответствующей иерархии. С помощью этих меток уровни классификации должны присваиваться субъектам и объектам;

б) при вводе новых данных в систему метка этих данных запрашивается и принимается от уполномоченного пользователя;

в) при наличии полномочий на перечисление пользователей новой организации она сравнивается с классификационными метками;

г) Предписанный принцип контроля доступа должен быть реализован для всех объектов с явным и скрытым доступом любого из субъектов. "Явный" здесь относится к доступу, сделанному с помощью системных инструментов - системных макросов, высокоуровневых языковых инструкций и т. д., в то время как "скрытый" относится к другому доступу, в том числе с использованием собственных программ устройств;

д) субъект может читать объект только в том случае, если иерархическая классификация на уровне классификации субъекта не меньше иерархической классификации на уровне классификации объекта;

е) субъект записывает объект только в том случае, если уровень классификации субъекта в иерархической классификации не превышает уровень классификации объекта в иерархической классификации;

ж) должна быть возможность изменения уровней классификации субъектов и объектов специально выделенными субъектами.

Для реализации дискреционного разграничения полномочий доступа отдельных категорий пользователей одного уровня в «закрытом» контуре должна применяться матричная модель контроля доступа субъектов к защищаемым объектам ТРД. Она должна:

– храниться в отдельном файле отдельного каталога. Полное имя и путь данного файла должны задаваться в консоли АИБ «закрытого» контура;

– содержать перечисление санкционированных (разрешенных) операций для каждой пары «субъект–объект» системы защиты. Должно быть задано явное и недвусмысленное перечисление допустимых типов доступа: читать, писать, удалять, запускать, переименовывать, т. е. тех типов доступа, которые являются санкционированными для данного субъекта к данному ресурсу (объекту).

Управление мандатным и дискреционным доступом субъектов в «закрытом» контуре к объектам контура – через доверенного диспетчера доступа (далее – доверенный диспетчер). При этом доверенный диспетчер должен обеспечить выполнение следующих задач:

а) присваивают пользователям домена и группам любые встроенные функциональные роли или роли безопасности в прикладном программном обеспечении "замкнутого" цикла или лишают их перечисленных ролей;

б) устанавливает права разграничения доступа субъектов «закрытого» контура к объектам, контролируемым прикладным программным обеспечением;

в) аудит успешных/или неудачных попыток идентификации, аутентификации и авторизации пользователей в специальном программном обеспечении «закрытого» контура, а также включение/отключение аудита событий выхода или прерывания сеанса пользователей прикладного программного обеспечения «закрытого» контура;

г) аудит успешных и/или неудачных попыток доступа отдельных субъектов «закрытого» контура (пользователей домена, групп или всех) к отдельным объектам, управляемым прикладным программным обеспечением на дискретной основе;

д) аудит успешных и/или неудачных попыток доступа к объектам, управляемым прикладным программным обеспечением пользователями в соответствии с мандатом, а также запрашиваемых прав доступа к объекту;

е) аудит успешных и/или неудачных попыток пользователей реализовать права в процессе работы с прикладным программным обеспечением;

ж) включение/отключение аудита событий блокировки/разблокировки операций прикладного ПО, а также изменений пользователей домена или полномочий групп в прикладном программном обеспечении (их включение/исключение из определённых функциональных ролей и/или ролей безопасности прикладного ПО);

з) задавать полное имя и путь к файлу, содержащему ТРД субъектов «закрытого» контура к объектам, управляемым прикладным ПО;

и) выполнять операции блокировки/разблокировки работы специального ПО.

Доверенный диспетчер должен регистрировать в журнале безопасности ОС следующие события, которые должны быть доступны для аудита:

– успешные и/или неудачные попытки идентификации, аутентификации и авторизации пользователей в прикладном ПО;

– выход или прерывание сеанса работы пользователя в прикладном ПО;

– успешные и/или неудачные попытки доступа к объектам, управляемым прикладным ПО, со стороны пользователей по дискреционному принципу;

– успешные и/или неудачные попытки верификации пользователей при выполнении тех или иных действий в системе;

– успешные и/или неудачные попытки назначение доменным пользователям или группам тех или иных встроенных функциональных ролей безопасности в прикладном ПО с консоли администрирования «закрытого» контура;

– события блокировки/разблокировки работы прикладного ПО;

– критические и фатальные ошибки, возникающие в программном коде доверенного диспетчера без возможности его отключения;

– успешные и/или неудачные попытки доступа к объектам со стороны пользователей по мандатному признаку;

– запрашиваемые права доступа к объекту.

При записи событий в журнале должны фиксироваться

– код (ID) события;

– тип события (успех, неудача);

– категория события («начало сеанса работы», «прекращение сеанса работы», «доступ к объектам», «применение полномочий», «изменение полномочий», «блокировка работы прикладного ПО», «разблокировка работы прикладного ПО», «критическая ошибка», «фатальная ошибка»);

– дата и время события;

– источник события;

– пользователь, инициировавший данное событие;

– компьютер, на котором инициировано данное событие;

описание события.

Администрирование доступом субъектов «закрытого» контура к защищенным объектам должно быть реализовано с помощью отдельной оснастки, консоли либо утилиты администрирования «закрытого» контура, представляющая собой отдельный файл, в котором должны быть реализованы возможности:

– разграничения доступа доменных пользователей и групп к объектам «закрытого» контура с учетом явного или косвенного (через несколько вложений в группы) включения пользователя во все группы, которым разрешен или явно запрещен доступ к указанному объекту с возможностью блокировки доступа в случае его запрета (дискреционный принцип);

– выдачи мандатных меток объектов, управляемых прикладным ПО «закрытого» контура;

– назначения отдельным пользователям или группам пользователей встроенных ролей прикладного ПО;

– регламентации доступа пользователей к физическим устройствам АРМ (дискам, портам ввода-вывода);

– разграничения доступа к маршрутизаторам и к серверам «закрытого» контура на уровне сетевых служб и процессов, обеспечивающих доступ к сетевым ресурсам по следующим параметрам:

а) пользователям;

б) процессам;

в) времени доступа;

г) по службам доступа (портам);

д) политике безопасности (запрещенные/разрешенные сервера и службы).

– создания замкнутой программной среды разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках АРМ «закрытого» контура. Управление замкнутой программной средой должно осуществляться централизованно;

– контроля целостности модулей системы защиты, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам АИБ «закрытого» контура:

а) контроль целостности должен выполняться по контрольным суммам, как в процессе загрузки, так и динамически;

б) механизм верификации контрольных сумм должен использовать аттестованный алгоритм;

в) анализ контрольных сумм должен проводиться как в процессе загрузки, так и динамически.

– оперативного восстановления средств защиты от НСД после сбоев и отказов оборудования в штатном режиме работы;

– регистрации всех действий пользователя в защищенном журнале «закрытого» контура с учетом наличия нескольких уровней регистрации;

– оповещения АИБ «закрытого» контура обо всех событиях НСД, происходящих в «закрытом» контуре.

3.2.2. Требования к криптографической подсистеме

Подсистема защиты криптографической информации предназначена для обеспечения конфиденциальности, целостности и авторизации информации, хранящейся, передаваемой и обрабатываемой в замкнутом контуре.

Подсистема криптографической защиты информации обеспечивает выполнение функций шифрования согласно ГОСТ 28147-89 и формирование/проверку электронной цифровой подписи (далее – ЭЦП). Следует использовать только стандартизированные алгоритмы цифровой подписи.

Подсистема защиты криптографической информации должна включать в себя компонент управления и распространения ключевой информации, а также компоненты, работающие на объектах управления, серверах и рабочих станциях администраторов и операторов ИС.

Компонент управления и распространения ключевой информации подсистемы криптографической защиты информации должен включать в себя формирование ключевых элементов шифрования и ЭЦП.

Подсистема криптографической защиты информации должна обеспечивать:

– шифрование всей секретной информации, которая записывается на совместно используемых различными субъектами носителей доступа (разделенных) данных, а также на съемных портативных носителях данных (дискетах, компакт-дисках, флэш-носителях и т.д.) долговременной внешней памяти для хранения вне сеансов уполномоченных субъектов доступа. Необходимо выполнить принудительную очистку областей внешней памяти,

содержащих ранее незашифрованную информацию. Доступ субъектов к операциям шифрования и соответствующим криптографическим ключам должен далее контролироваться подсистемой управления доступом. Порядок работы с ключевыми материалами криптографических систем защиты информации регулируется;

– использование различных ключей шифрования для групп пользователей в соответствии с их полномочиями для доступа к защищенным ресурсам при использовании криптографических средств для контроля доступа уполномоченных пользователей к информационным ресурсам «закрытого» контура. Ключи шифрования должны быть защищены;

– формирование и проверка ЭЦП;

– формирование ключевых элементов шифрования для пользователей «закрытого» контура ЛВС, пользователей «открытого» контура и для пользователей «закрытых» контуров взаимодействующих систем ведомственных сегментов;

– управление ключевой информацией и ее распространение;

– криптографическую стойкость и многоуровневую защиту от компрометации ключевой информации, разделение пользователей по уровням защиты и областям их взаимодействия между собой и пользователями других уровней;

– криптографическую защиту межсетевого обмена между ЛВС «закрытого» контура и взаимодействующими системами ведомственных сегментов. Информация должна быть зашифрована перед отправкой по сети. При передаче секретной информации на носителе - перед записью на носитель.

– раздельное шифрование всей конфиденциальной информации, которая записывается на совместно используемую различными субъектами внешнюю память, а также на съемных носителях данных (компакт-дисках, носителях USB и т. д.

– принудительную очистку участков внешней памяти, содержащих ранее незашифрованную информацию. Доступ субъектов к операциям шифрования и соответствующим криптографическим ключам должен контролироваться подсистемой управления доступом и др.

Должны использоваться сертифицированные средства криптографической защиты.

3.2.3. Подсистема контроля целостности «закрытого» контура

Подсистема контроля целостности «закрытого» контура должна обеспечивать контроль:

– файлов операционной системы до ее загрузки;

– изменения файлов;

– создания и удаления файлов;

– переименования файлов;

– создания и удаления каталогов;

– переименования файлов;

– перемещения файлов из каталога в каталог;

– содержимого системных областей.

Подсистема должна запускаться автоматически при инициализации аппаратно-программных средств «закрытого» контура, а также в ручном режиме.

Контроль целостности должен осуществляться путем:

– перехвата обращений к функциям ОС работы с файловой системой и задания перечня разрешенных действий;

– сравнения зафиксированного эталонного состояния объектов с их текущим состоянием. Фиксация эталонного состояния контролируемых объектов должна осуществляться путем создания эталонных копий, хранение которых осуществляется в защищенных областях жесткого диска или на защищенных внешних носителях.

Подсистема должна иметь удобный пользовательский интерфейс для создания списка контролируемых объектов с помощью масок, шаблонов и поисковой системы.

Контроль целостности должен осуществляться в соответствии с контрольными суммами как во время загрузки, так и динамически. Механизм проверки контрольной суммы должен использовать сертифицированный алгоритм. Анализ контрольной суммы должен выполняться как во время загрузки, так и динамически.

Защита должна включать в себя процедуру восстановления от отказов и отказов оборудования, которая должна обеспечивать восстановление свойств.

Должен быть реализован механизм восстановления работоспособности средств защиты в случае нарушений в его нормальном режиме работы. Функциональность должна быть восстановлена сразу после обнаружения сбоя в нормальной работе.

3.2.4. Подсистема защиты межсетевого взаимодействия «закрытого» контура

Подсистема защиты межсетевого взаимодействия, закрытого «закрытого» контура предназначена для защиты однонаправленной передачи данных из «открытого» контура в «закрытый» контур и сегментирования ЛВС указанных контуров.

Подсистема защиты межсетевого взаимодействия, закрытого «закрытого» контура должна обеспечивать:

1. Сегментацию ЛВС «закрытого» контура и ЛВС «открытого» контура на канальном, сетевом и прикладном уровнях семиуровневой модели OSI. Управление потоками между ЛВС «закрытого» контура и ЛВС «открытого» контура обеспечивается:

а) однонаправленной фильтрацией потока данных между «открытым» контуром и «закрытым» контуром;

б) фильтрацией на канальном уровне, а именно:

– фильтрацией потока данных на основе MAC-адресов отправителя и получателя;

– фильтрацией средствами защиты с учетом входного и выходного сетевого интерфейса и проверкой подлинности сетевых адресов. В настройках параметров фильтрации должна присутствовать возможность допускать или – запрещать прохождение сетевыми пакетами из списка адресов указанный сетевой интерфейс;

– фильтрацией с учетом даты/времени и возможности определения временных интервалов для выполнения правил фильтрации.

в) фильтрация на сетевом уровне, а именно:

– фильтрацией каждого сетевого пакета независимо на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. Фильтрация производится по IP-адресам и MAC-адресам;

– фильтрацией на межсетевых экранах с учетом любых значимых полей сетевых пакетов;

– фильтрацией пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств «закрытого» контура. Должна обеспечиваться поддержка фильтрации протокола ICMP;

– фильтрацией с учетом даты/времени и возможность определения временных интервалов для выполнения правил фильтрации;

– регистрацией и учетом фильтруемых пакетов. В параметры регистрации должны включаться адрес, время и результат фильтрации.

г) фильтрация на транспортном уровне, а именно:

– фильтрацией запросов на установление виртуальных соединений. При этом должны учитываться транспортные адреса отправителя и получателя. Фильтрация должна производиться по IP-адресам для TCP и UDP соединений;

– фильтрацией с учетом даты/времени и возможности определения временных интервалов для выполнения правил фильтрации;

регистрацией и учетом запросов на установление виртуальных соединений.

д) фильтрация на прикладном уровне, а именно:

– фильтрацией на прикладном уровне запросов к прикладным сервисам. При этом должны учитываться прикладные адреса отправителя и получателя; Фильтрация производится по сокетам (sockets) для TCP и UDP соединений;

– возможностью сокрытия субъектов (объектов) и/или прикладных функций «закрытого» контура;

– фильтрацией с учетом даты/времени и возможности определения временных интервалов для выполнения правил фильтрации;

– регистрацией и учетом запрашиваемых сервисов прикладного уровня (посредством связки IP-адреса и номера порта удаленного сервера для устанавливаемого сеанса связи).

2. Авторизация MAC-адресов АРМ пользователей с «закрытым» контуром при подключении к локальной сети с «закрытым» контуром. При обнаружении неавторизованного MAC-адреса порт соответствующего устройства должен быть автоматически отключен.

3. Использует режим концентратора, который принимает пакеты, адресованные только авторизованному MAC-адресу.

4. Исключить и контролировать доступ к несанкционированным удаленным подключениям к локальным ресурсам «закрытого» контура.

5. Обязательный мониторинг открытых точек доступа к периметру «закрытого» контура. При организации однонаправленных соединений из «открытого» контура в «закрытый» контур для обеспечения доступа к секретной информации, обрабатываемой на серверах «закрытого» контура, необходимо заранее решить вопрос криптографической защиты трафика этих соединений с помощью сертифицированных средств ФСБ России. В то же время для разрешенных TCP-соединений, исходящих из «открытого» контура, необходимо указать адрес назначения, адрес источника и номер IP-порта, соответствующие службе, внешней для «открытого» контура.

6. Регистрация входящих пакетов в «закрытый» контур, не соответствующих правилам листов доступа маршрутизатора и внутреннего МЭ, путем отображения соответствующих событий в системном журнале.

7. Контроль информации, передаваемой через электронную систему обмена сообщениями в «закрытом» контуре путем фильтрации протоколов передачи электронной почты специализированными средствами, установленными на серверах, обеспечивающих работу почтовой системы внутри «закрытого» контура. Правила фильтрации должны регулироваться. Рабочие данные фильтра передаются в подсистему управления безопасностью.

8. Программируемый ответ на события в устройстве защиты (возможность генерировать заданный уровень детализации событий в журнале АИБ. Регистрация категорий событий, таких как изменение конфигурации и т.д.).

9. Оперативная сигнализация на основе защищенного протокола SNMP v.3, а именно:

– локальная сигнализация попыток нарушения правил фильтрации (оповещение АИБ «закрытого» контура о попытках установления запрещенных соединений непосредственно фильтрующим модулем (звуковое сопровождение, вывод сообщения на экран, световая индикация и т.п.));

– дистанционная сигнализация попыток нарушения правил фильтрации (информирование АИБ «закрытого» контура и уполномоченных лиц о попытках установления запрещенных соединений с помощью электронной почты, SMS-сообщений или внешних систем оповещения).

3.2.5. Подсистема администрирования «закрытого» контура

Подсистема администрирования «закрытого» контура предназначена для настройки прав разграничения доступа (далее – ПРД) субъектам

«закрытого» контура к объектам управления. В «закрытом» контуре должна быть реализована централизованная подсистема администрирования СЗИ «закрытого» контура.

Управление активным сетевым оборудованием «закрытого» и «открытого»контуров ЛВС ИС должно контролироваться специалистами отдела информационной безопасности с использованием механизмов регулярного аудита сетевого оборудования. Подсистема аудита должна управляться подразделениями информационной безопасности.

Администрирование СЗИ «закрытого» контура должно производиться АИБ «закрытого» контура с локальной консоли или удаленно с использованием шифрования трафика управления на IP-уровне или с использованием протоколов управления с поддержкой шифрования данных (SNMP v3). Удаленные запросы безопасности должны использовать методы, устойчивые к пассивному и активному перехвату информации. Для этого следует использовать криптографические механизмы аутентификации с использованием ЭЦП.

В подсистеме администрирования должна быть реализована система агентов, для всех защищенных АРМ, позволяющая АИБ «закрытого» контура в реальном времени получать информацию и осуществлять централизованное управление политикой безопасности системы защиты.

Подсистема администрирования должна обеспечивать:

– установку ключевых элементов и механизмов доступа в средства СЗИ «закрытого» контура с целью обеспечения им возможности доступа к объектам управления. При этом установка и перестановка ключевых элементов и механизмов доступа должна осуществляться как по команде администратора центра генерации и распространения ключей (ЦГРК), так и по инициативе администратора «закрытого» контура;

– взаимодействие с ЦГРК с целью обеспечения доставки ключевых элементов и механизмов доступа;

– установку ПРД и их изменение;

– идентификацию и аутентификацию АИБ «закрытого» контура при его запросах на доступ;

– возможность делегирования прав (т. е. присвоения пользователю ограниченных административных привилегий управления некоторым набором учетных записей);

– использование универсальных шаблонов настроек политики безопасности «закрытого» контура;

– возможность моделирования существующей организационной иерархии и административной структуры «закрытого» контура – пользователя «закрытого» контура;

– возможность блокировки учетной записи пользователя «закрытого» контура или её ограничения по времени работы;

– возможность доставки информации о нештатных ситуациях и ошибках, возникающих в процессе функционирования механизмов доступа, до АИБ «закрытого» контура.

3.2.6. Подсистема обнаружения и противодействия вторжений

Подсистема обнаружения и противодействия вторжений должна обеспечивать:

– удаленный централизованный, автоматизированный контроль функционирования процессов создания, обработки, хранения и передачи информации в рамках «закрытого» контура;

– контроль за вычислительной средой объектов «закрытого» контура, в которой выполняются прикладные задачи;

– контроль правильности работы прикладного программного обеспечения «закрытого» контура, реализующего функции обработки информации;

– контроль правильности работы операторов и администраторов «закрытого» контура.

3.2.7. Подсистема мониторинга информационной безопасности «закрытого» контура

Подсистема мониторинга информационной безопасности «закрытого» контура предназначена для оперативного контроля ее стояния с целью выявления нарушений требований политики ИБ «закрытого» контура и нормативных документов, выявления нештатных (или злоумышленных) действий и локализации инцидентов безопасности. Регистрация и анализ данных аудита должна производится централизованно на серверах (машинах) безопасности (далее – МБ) в режиме реального времени в соответствии с заданной политикой безопасности.

Подсистема аудита ИБ «закрытого» контура должна обеспечивать:

– контроль выполнения требований политики ИБ «закрытого» контура и нормативных документов по ИБ;

– независимый мониторинг действий пользователей «закрытого» контура;

– сбор первичных событий штатных журналов аудита объектов мониторинга, в том числе СЗИ;

– регистрацию первичных событий аудита;

– анализ первичных событий аудита в реальном времени и фиксацию событий ИБ на основе правил анализа событий ИБ от разнотипных источников «закрытого» контура;

– обеспечение возможности создания и редактирования, а также проверки описаний событий ИБ;

– обеспечение централизованного хранения зафиксированной информации о событиях ИБ и их последующий (отложенный) анализ (разбор

событий аудита, выявление цепочек операций, выполняемых на серверах, рабочих станциях администраторов и операторов «закрытого» контура;

– формирование сообщений о событиях ИБ и извещения персонала службы ИБ о зафиксированных событиях ИБ;

– расследование событий ИБ и регистрацию инцидентов ИБ.

3.3. Подсистема защиты информации «открытого» контура

Целевые функции защиты «открытого» контура должны быть реализованы в следующих функциональных подсистемах защиты информации «открытого» контура:

– защиты информации от НСД;

– защиты межсетевого взаимодействия «открытого» контура;

– администрирования.

Основные требования к подсистемам «открытого» контура приведены в [17].

3.3.1. Подсистема защиты информации от НСД «открытого» контура

Подсистема защиты информации от НСД «открытого» контура предназначена для предназначена для организации сегментации и защиты информации, передаваемой между «открытого» контура и «открытыми» контурами взаимодействующих ИС по открытым каналам, включая Интернет.

Подсистема защиты информации от НСД «открытого» контура должна обеспечивать:

– разграничение доступа к маршрутизаторам и к серверам «открытого» контура на уровне сетевых служб и процессов, обеспечивающих доступ к сетевым ресурсам по следующим параметрам:

а) пользователям;

б) процессам;

в) времени доступа;

г) по службам доступа (портам);

д) политике безопасности (запрещенные/разрешенные сервера и службы);

– контроль удаленного доступа на выделенном сервере аутентификации «открытого» контура, на котором должны поддерживаться следующие функциональные возможности:

а) согласование используемых протоколов аутентификации и отсутствие жесткой привязки к конкретным протоколам аутентификации;

б) блокирование любых попыток обхода фазы аутентификации после установления удаленного соединения;

в) аутентификация каждой из взаимодействующих сторон - как удаленного пользователя, так и сервера удаленного доступа, что исключает возможность маскировки как одного из участников взаимодействия;

г) выполнение не только начальной аутентификации до допуска к ресурсам ЛВС с "открытым" контуром, но и динамической аутентификации взаимодействующих сторон при работе удаленного соединения;

д) использование одноразовых паролей или криптографическая защита передаваемых секретных паролей, исключающая возможность повторного использования перехваченной информации для ложной аутентификации;

– усиленную аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети;

– разграничение доступа к маршрутизаторам и к серверам «открытого» контура на уровне сетевых служб и процессов, обеспечивающих доступ к сетевым ресурсам по следующим параметрам:

а) пользователям;

б) процессам;

г) времени доступа;

д) по службам доступа (портам);

е) политике безопасности (запрещенные/разрешенные сервера и службы);

– однозначную идентификацию пользователей в ИС и в операционной системе ОС АРМ (использование общих идентификаторов (ни в СЗИ, ни в ОС) не допускается;

– идентификацию по логическим именам информационных ресурсов (логических устройств, каталогов, файлов);

– исключение возможности удаленного подключения к локальным ресурсам «открытого» контура и управление доступом к этим ресурсам за счет настроек ОС;

– дискреционное (одноуровневое) разграничение доступа с помощью ТРД. Для реализации дискреционного разграничения полномочий доступа отдельных категорий пользователей одного уровня в «открытом» контуре должна применяться матричная модель контроля доступа субъектов к защищаемым объектам:

а) ТРД должна храниться в отдельном файле отдельного каталога. Полное имя и путь данного файла должны задаваться в консоли АИБ «открытого» контура;

б) ТРД должна содержать перечисление санкционированных (разрешенных) операций для каждой пары «субъект–объект» системы защиты «открытого» контура. Должно быть задано явное и недвусмысленное перечисление допустимых типов доступа: читать, писать, удалять, запускать, переименовывать, т. е. тех типов доступа, которые являются санкционированными для данного субъекта к данному ресурсу (объекту);

– управление дискреционным доступом субъектов в «открытом» контуре к объектам контура через доверенного диспетчера доступа. При этом доверенный диспетчер должен выполнять следующие задачи:

а) установление прав на разграничение доступа субъектов к объектам;

б) аудит успешных/или неудачных попыток идентификации, аутентификации и авторизации пользователей в "разомкнутом" цикле;

в) включение/выключение аудита событий выхода или прерывания сеанса пользователей в "открытом" контуре и "открытом" контуре;

г) аудит успешных и/или неудачных попыток доступа отдельных объектов в "разомкнутом" цикле (пользователей домена, групп или всех) к отдельным объектам на дискреционной основе;

д) аудит успешных и/или неудачных попыток доступа к объектам в "разомкнутом" цикле;

е) аудит запрошенных прав доступа к объекту в "разомкнутом" цикле;

и) постановку на аудит успешные и/или неудачные попытки пользователей использовать привилегии в процессе эксплуатации объектов "открытого" контура;

к) включение/отключение аудита событий блокировки/разблокировки работы прикладного программного обеспечения в "разомкнутом" контуре;

л) включение/отключение аудита изменений прав пользователей домена или групп в прикладном программном обеспечении;

м) указание полного имени и пути файла, содержащего ТРД субъектов «открытого» контура к объектам, управляемым прикладным программным обеспечением;

н) выполнение операции блокировки/разблокировки работы прикладного программного обеспечения;

– администрирование доступом субъектов «открытого» контура к объектам должно быть реализовано с помощью отдельной оснастки, консоли либо утилиты администрирования АИБ «открытого» контура, представляющая собой отдельный файл, в которой должна быть реализована возможность:

а) разграничения доступа доменных пользователей и групп к объектам «открытого» контура с учетом явного или косвенного (через несколько вложений в группы) включение пользователя во все группы, которым разрешен или явно запрещен доступ к указанному объекту с возможностью блокировки доступа в случае его запрета (дискреционный принцип);

б) назначения отдельным пользователям или группам пользователей встроенных ролей прикладного ПО;

– регламентацию доступа пользователей к физическим устройствам АРМ (дискам, портам ввода-вывода);

– создание замкнутой программной среды разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках АРМ «открытого» контура. Управление замкнутой программной средой в «открытом» контуре должно осуществляться централизованно;

– контроль целостности модулей системы защиты «открытого» контура, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам АИБ «открытого» контура:

а) контроль целостности должен выполняться по контрольным суммам, как в процессе загрузки, так и динамически;

б) механизм верификации контрольных сумм должен использовать аттестованный алгоритм;

в) анализ контрольных сумм должен проводиться как в процессе загрузки, так и динамически;

– оперативное восстановление средств защиты от НСД после сбоев и отказов оборудования в штатном режиме работы;

– оповещение АИБ «открытого» контура обо всех событиях НСД, происходящих в «открытом» контуре.

Доверенный диспетчер должен регистрировать в журнале безопасности ОС следующие события, которые должны быть доступны для аудита:

– успешные и/или неудачные попытки идентификации, аутентификации и авторизации пользователей в прикладном ПО;

– выход или прерывание сеанса работы пользователя в прикладном ПО;

– успешные и/или неудачные попытки доступа к объектам, управляемым прикладным ПО, со стороны пользователей по дискреционному принципу;

– успешные и/или неудачные попытки верификации пользователей при выполнении тех или иных действий в системе;

– успешные и/или неудачные попытки назначение доменным пользователям или группам тех или иных встроенных функциональных ролей безопасности в прикладном ПО с консоли администрирования «открытого» контура;

– события блокировки/разблокировки работы прикладного ПО;

– критические и фатальные ошибки, возникающие в программном коде доверенный диспетчер без возможности его отключения;

– успешные и/или неудачные попытки доступа к объектам со стороны пользователей по мандатному признаку;

– запрашиваемые права доступа к объекту.

При записи событий в журнале должны фиксироваться:

– код (ID) события;

– тип события (успех, неудача);

– категория события («начало сеанса работы», «прекращение сеанса работы», «доступ к объектам», «применение полномочий», «изменение полномочий», «блокировка работы прикладного ПО», «разблокировка работы прикладного ПО», «критическая ошибка», «неустранимая ошибка»);

– дата и время события;

– источник события;

– пользователь, инициировавший данное событие;

– компьютер, на котором инициировано данное событие;

описание события.

3.3.2. Подсистема защиты межсетевого взаимодействия «открытого» контура

Подсистема защиты межсетевого взаимодействия «открытого» контура предназначена для защиты и управления потоками данных между ЛВС «открытого» контура ИС организации и ЛВС «открытых» контуров ее удаленных филиалов через сети общего пользования (сети Интернет, мобильные сети 2G, 3G, 4G и д. р.).

Подсистема защиты межсетевого взаимодействия, открытого «открытого» контура должна обеспечивать:

– контролируемый доступ межсетевого взаимодействия «открытого» контура с системами открытых сегментов ИС через внешние «демилитаризованные зоны». Внешняя «демилитаризованная зона» должна содержать а) сервер доступа для внешних пользователей систем; б) сервер авторизации внешних пользователей систем. Любой внешний доступ к ресурсам, расположенным в «открытом» контуре за пределами «демилитаризованных зон», должен быть запрещен. «Демилитаризованная зона» должна быть подключена непосредственно к внешнему брандмауэру (МЭ). Внешние пользователи должны иметь доступ к серверам «открытого» контура, выделенным в отдельный сегмент, через строго определенный набор протоколов связи и приложений с использованием прокси-механизмов. Внешним сетевым экраном должны быть МЭ, работающие на маршрутизаторах, а именно сетевые фильтры и средства управления доступом, встроенные в операционную систему;

– обеспечение доступа внешних взаимодействующих системам только к ресурсам «демилитаризованных зон» «открытого» контура по строго определенному набору коммуникационных и прикладных протоколов;

– управление всеми внешними экранами в части настроек параметров безопасности;

– фильтрацию на внешних МЭ и маршрутизаторах на принципе «все, что не разрешено, то запрещено». Критерии фильтрации могут быть основаны на применении одного или нескольких правил фильтрации;

– программируемый ответ на события в средстве защиты (возможность генерировать заданный уровень детализации событий в журнале администратору информационной безопасности. Регистрация категорий событий, таких как установка связи, изменение конфигурации и т.д.)

– оперативную сигнализацию на основе защищенного протокола SNMPv.3:

а) локальная сигнализация попыток нарушения правил фильтрации (АИБ «открытого» контура о попытках установления запрещенных соединений непосредственно модулем фильтрации (аудиотрекинг, вывод сообщения на экран, световая индикация и т. д.);

б) дистанционная сигнализация попыток нарушения правил фильтрации (информирование АИБ «открытого» контура и уполномоченных лиц ИС о попытках установления запрещенных соединений с помощью электронной

почты, пейджинговой услуги, SMS-сообщений или внешних систем предупреждения);

– контроль отсутствия пакетов в/из «открытого» контура, не соответствующих правилам access-листов маршрутизатора и внешнего МЭ за счет вывода в syslog соответствующих событий;

–контроль информации, передаваемой через систему электронной почты, путем фильтрации протоколов передачи электронной почты специализированными средствами, установленными на серверах, обеспечивающих работу почтовой системы внутри ИС. Правила фильтрации должны регулироваться. Рабочие данные фильтра передаются в подсистему управления безопасностью.

– управление потоками между ЛВС «открытого» контора и системами внешних взаимодействующих сегментов ИС осуществляется фильтрацией на *сетевом уровне*, а именно:

а) фильтрация для каждого сетевого пакета независимо на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. Фильтрация основана на IP-адресах и MAC-адресах;

б) фильтрация на брандмауэрах с учетом любых значимых полей сетевых пакетов;

в) фильтрация пакетов протокола службы, используемых для диагностики и управления работой сетевых устройств. Должна поддерживаться фильтрация ICMP;

г) возможность преобразования сетевых адресов на брандмауэрах. Должно быть реализовано использование маскирующей функции, предполагающей режим модификации проходящих пакетов от субъекта «открытого» контура в систему внешних взаимодействующих сегментов ИС. IP-адрес субъекта (отправителя) изменяется на адрес внешнего сетевого интерфейса внутреннего брандмауэра. При получении ответа на сообщение, посланное данным субъектом, должна происходить обратная процедура;

д) фильтрацию на основе даты/времени и возможность определения временных интервалов для выполнения правил фильтрации;

е) регистрация и учет отфильтрованных пакетов. Параметры регистрации должны включать адрес, время и результат фильтрации;

– управление потоками между ЛВС «открытого» контора и системами внешних взаимодействующих сегментов ИС осуществляется фильтрацией на *транспортном уровне*, а именно:

а) фильтрация запросов на установление виртуальных соединений. Необходимо учитывать адреса доставки отправителя и получателя. Фильтрация должна основываться на IP-адресах для соединений TCP и UDP;

б) фильтрация даты/времени и возможность определения временных интервалов для выполнения правил фильтрации;

г) регистрация и учет запросов на установление виртуальных соединений;

– управление потоками между ЛВС «открытого» контора и системами внешних взаимодействующих сегментов ИС осуществляется построением *защищенных виртуальных сетей*(Virtual Private Network, VPN) с возможностью осуществлять централизованное управление компонентами VPN, а именно:

а) должна быть реализована архитектура клиент-сервер, включающая центр управления компонентами VPN;

б) должно быть реализовано централизованное управление конфигурацией компонента VPN (механизм удаленной конфигурации);

в) дистанционная настройка должна осуществляться по защищенному каналу с аутентификацией абонентов канала;

г) осуществляется централизованное распространение криптографических ключей на основе сертификационного органа;

д) должен быть реализован графический интерфейс для создания и модификации профилей конфигурации VPN;

е) должна быть реализована возможность создания резервной копии конфигурации VPN;

ж) должен обеспечиваться непрерывный мониторинг функций защиты агентами, установленными на рабочих станциях и серверах VPN.

3.3.3. Подсистема администрирования «открытого» контура

Подсистема администрирования «открытого» контура предназначена для настройки прав разграничения доступа (далее – ПРД) субъектам «открытого» контура к объектам управления. В «открытом» контуре должна быть реализована централизованная подсистема администрирования СЗИ «открытого» контура, осуществляемая АИБ «открытого» контура с локальной консоли либо удаленно. Подсистема администрирования должна быть реализована на базе системы агентов для всех АРМ, которая позволит АИБ «открытого» контура получать информацию в режиме реального времени и централизованно управлять политикой защиты. Подсистема администрирования должна обеспечивать:

– установку ПРД и их изменение;

– идентификацию и аутентификацию АИБ «открытого» контура при запросах доступа;

– возможность делегирования прав (т. е. присвоения пользователю ограниченных административных привилегий управления некоторым набором учетных записей);

– использование универсальных шаблонов настроек политики безопасности «открытого» контура;

– возможность моделирования существующей организационной иерархии и административной структуры «открытого» контура – пользователя «открытого» контура;

– возможность блокировки учетной записи пользователя «открытого» контура или ограничения времени ее работы;

– возможность доставки информации о нештатных ситуациях и ошибках, возникающих в процессе функционирования механизмов доступа, до АИБ «открытого» контура.

Примечание.

Для обеспечения должного уровня защиты информации при использовании технологии виртуализации в «открытом» контуре ИС дополнительные организационные и технические меры, применяемые для защиты среды виртуализации, должны обеспечивать в соответствии с требованиями ГОСТ Р 57580.1—2017:

– организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации;

– организацию и контроль информационного взаимодействия и изоляции виртуальных машин;

– организацию защиты образов виртуальных машин;

– регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.

Контрольные вопросы по гл. 3

1. Какие общие требования информационной безопасности предъявляются к построению защищенных сегментов «закрытого» и «открытого» контуров ЛВС ИС?
2. Какие требования информационной безопасности предъявляются к подсистеме резервирования и восстановления информации в ИС?
3. Какие требования информационной безопасности предъявляются к подсистеме контроля эталонного состояния информации и рабочей среды в ИС?
4. Какие требования информационной безопасности предъявляются к подсистеме управления безопасностью в ИС?
5. Какие требования информационной безопасности предъявляются к подсистеме защиты информации от НСД «закрытого» контура ИС?
6. Какие требования информационной безопасности предъявляются к подсистеме криптографической защиты информации «закрытого» контура?
7. Какие требования информационной безопасности предъявляются к подсистеме антивирусной защиты информации «закрытого» контура?
8. Какие требования информационной безопасности предъявляются к подсистеме контроля целостности «закрытого» контура?
9. Какие требования информационной безопасности предъявляются к подсистеме защиты межсетевого взаимодействия «закрытого» контура?
10. Какие требования информационной безопасности предъявляются к подсистеме администрирования «закрытого» контура?

11. Какие требования информационной безопасности предъявляются к подсистеме обнаружения и противодействия вторжений «закрытого» контура?
12. Какие требования информационной безопасности предъявляются к подсистеме аудита состоянии ИБ «закрытого» контура?
13. Какие требования информационной безопасности предъявляются к подсистеме защиты информации от НСД «открытого» контура?
14. Какие требования информационной безопасности предъявляются к подсистеме антивирусной защиты информации «открытого» контура?
15. Какие требования информационной безопасности предъявляются к подсистеме защиты межсетевого взаимодействия «открытого» контура?
16. Какие требования информационной безопасности предъявляются к средствам построения защищенных виртуальных сетей (VPN)?
17. Какие требования информационной безопасности предъявляются к подсистеме администрирования «открытого» контура?
18. Что должны обеспечивать организационно-технические меры, применяемые для защиты среды виртуализации «открытого» контура?

Глава 4. Организационно-технические предложения по методам и механизмам защиты ИС организации

Для построения СИБ ИССоответствующего класса защищенности, должны быть выбраны защитные меры и механизмы защиты, реализующие требования Политики ИС и ведомственных документов организации, а также требований документов ФСТЭК [11-13] и других регуляторов. Выбор защитных мер, адекватных моделям угроз и нарушителей, должен проводится с учетом затрат на их реализацию и объема возможных потерь от реализации угроз. При этом должны применяться только те защитные меры, эффективность работы которых может быть проверена с учетом их на бизнес–цели.

Ниже приводятся общие подходы по защите «закрытого» и «открытого» контуров ИС организации [15-17].

4.1. Технические решения для защиты компьютерных ресурсов серверов и АРМ

4.1.1. Общие организационно-технические решения по обеспечению безопасности

В качестве приоритетной организационной меры по предотвращению потенциальных угроз со стороны группы администраторов необходимо сначала разделить полномочия по обеспечению доступа к управлению компонентов ИС и непосредственному управлению этими компонентами. Кроме того, необходимо ограничить доступ к оборудованию путем оснащения помещений средствами демилитаризации доступа.

Для предотвращения несанкционированного дистанционного сетевого управления оборудованием необходимо использовать средства фильтрации сетевого трафика, позволяющие управлять оборудованием только из выделенного для этих целей АРМ, указанный АРМ должен быть оснащен средствами защиты от НСД, обеспечивая, в частности, невозможность изменения её сетевых настроек (например, СЗИ от НСД SecretNet)

Пользователи и администраторы всех компонентов ИС должны иметь в них уникальные идентификаторы. Использование чужих идентификаторов должно быть запрещено. Учетные записи администратора этих систем (например, *root* в HP-UX, *SYS* в СУБД Oracle) должны использоваться только в том случае, если требуемая операция не может быть выполнена технически с использованием учетной записи индивидуального администратора этой системы.

При настройке инструментов регистрации событий на другой уровень детализации перехваченных событий в серверной ОС, сетевом оборудовании ОС, ОС АРМ и СУБД должны быть выполнены следующие требования.

1. Полнота зарегистрированных событий должна быть достаточной, а не избыточной для доказательного анализа ситуации.

2. Данные аудита должны быть максимально независимыми от администратора контролируемой системы.

3. Необходимо обеспечить несанкционированное искажение журналов аудита, включая системных администраторов.

4. Мониторы безопасности должны использоваться для быстрого обнаружения возможных атак в режиме реального времени.

5. Журналы аудита должны храниться в сроки, определенные правилами компании.

Вне зависимости от типа операционной системы, подсистема аудита должна обеспечивать регистрацию:

1. Идентификационная информация, включая попытки пользователей ввести пароль.

2. Операции, отклоненные автоматизированными системами из-за отсутствия полномочий операторов.

3. Факт модификации конфигурационных файлов IE.

4. Тот факт, что администраторы изменили разрешения пользователей.

5. Система аудита отключена администраторами.

6. Факты IE начинаются и останавливаются.

4.1.2. Решения по ОС HP-UX для обеспечения корпоративной безопасности

Для контроля за соблюдением принципов ИБ, описанных выше, для ОС HP-UX должен быть выполнен следующий набор работ.

1. Включить и настроить аудит ОС HP-UX:

1.1. Установить ОС HP-UX в режим Trusted HP-UX для расширенной аутентификации пользователей. Trusted HP-UX предоставляет следующие дополнительные функции управления учетными записями пользователей и паролями:

– зашифровывать файл паролей (*shadowed passwd file*);

– ограничить время пользователя, количество попыток входа в систему, пароль и срок действия учетной записи;

– требовать пароль от пользователя при входе в систему в одномодовом режиме (*single-mode*);

– настроить автоматическое отключение долгосрочных неиспользуемых учетных записей.

Для этого требуется войти в консоль сервера под именем *root* и использовать утилиту *sam* для выполнения необходимых действий. Затем необходимо перегрузить ОС путем ввода *shutdown –r now* с консоли.

1.2. Обеспечить невозможность неконтролируемого администрирования системы аудита ОС администратором ОС, для чего:

– запретить пользователю *root* работу в нормальном режиме, так как действия пользователя *root* не регистрируются в ОС. Это можно сделать, разделив пароль входа для *root*, ограничив доступ к файлу пароля ОС. После установки ОС разделите пароль *root* на две части, одна из которых

передается в административную группу ИС, а другая – в группу безопасности. Первоначальное разделение паролей и их изменение осуществляется их совместным набором администратором ИС и АИБ в соответствии с принятой политикой защиты паролей;

– создать учетные записи АИБ и, в дополнение к пользователю *root*, создать администратора ОС. Разделите свои разрешения, чтобы запретить АИБ настраивать ОС и администратору ОС доступ к журналам аудита. Обеспечить, чтобы администратор ОС и АИБ обладали необходимыми и достаточными полномочиями для выполнения своих функциональных обязанностей, запретив при этом АИБ вносить какие-либо изменения в настройки ОС, а администратору ОС – искажать журналы аудита для чего реализовать их перенос на сервер аудита безопасности в режиме реального времени;

– включить аудит всех команд, выполняемых администратором ОС HP-UX, а также аудит операций удаления/записи в файлы конфигурации системы HP-UX ОС и СУБД Oracle.

– с помощью штатных средств HP-UX запретить администратору ОС управление журналами аудита ОС, а именно: запретить ему доступ к командам *audsys, audusr, audevent audisp, audomon*, а также запись в каталог аудита. Администратор безопасности не должен изменять настройки HP-UX при сохранении возможности управления аудитом (права на выполнение команд для чтения и записи в файлы аудита).

1.3. Обеспечить оперативный контроль за аудиторской информацией, для чего:

– настройте параметры *syslogd* и аудита таким образом, чтобы информация аудита дублировалась на сервере аудита безопасности;

– включите аудит всех команд, выполняемых администратором HPUX, а также операций удаления/записи в файлы конфигурации системных настроек, например, ОС HP-UX и СУБД Oracle;

– поскольку система HP-UX не обеспечивает аудит пользователя *root*, используйте этот идентификатор только в том случае, если идентификатор администратора HP-UX не может быть использован.

1.4. Обеспечить оперативный анализ и периодическое архивирование аудиторской информации, а также порядок взаимодействия отделов по результатам анализа аудиторской информации.

Каталог для размещения файлов аудита необходимо поместить в отдельную файловую систему размером не менее 512 МБ, чтобы избежать переполнения диска в корневой файловой системе и отключения ОС. После этого ОС считается готовой к включению подсистемы аудита.

2. Оптимизировать набор сервисов и системного ПО на серверах, для чего:

2.1. Ограничьте набор услуг, загружаемых в ОС HP-UX, услугами, необходимыми для работы и администрирования ИС и систем резервного копирования. Также необходимо ограничить набор установленного

системного ПО только программными пакетами, необходимыми для работы ИС, в частности, не устанавливать компиляторы. Чтобы минимизировать риск безопасности серверов HP-UX, необходимо ограничить набор сервисов HP-UX, загружаемых ОС, только необходимыми для работы (табл. 4.1).

Таблица 4.1.

Минимальный набор сервисов необходимых для работы ОС HP-UX

Номер сервиса	Вид сервиса	Название сервиса
23	Tcp	telnet
53	Tcp	Domain
111	Tcp	Sunrpc
113	Tcp	authentication
135	Tcp/Udp	Unknown
177	Udp	Unknown
382	Tcp	Pvserver
512	Udp	Syslog
515	Tcp	Printer
543	Tcp	Klogin
544	Tcp	Kshell
806	Udp	Unknown
808	Tcp	Unknown
812	Tcp	Unknown
816	Tcp/Udp	Unknown
821	Tcp	Unknown
824	Tcp	Unknown
825	Tcp	Unknown
826	Udp	Unknown
827	Udp	Unknown
891	Udp	Unknown
1023	Udp	Unknown
2049	Udp	nfs
6112	Tcp	Dtsps

3. Обеспечить контроль целостности программных компонент и конфигурационных файлов ОС, а именно:

– файлов системных настроек (каталог /etc);

– всех исполняемых файлов и библиотек ОС;

– ядра операционной системы;

– файлов драйверов устройств (каталог /dev).

4. Обеспечить своевременное получение обновлений ОС (patches) от поставщиков ОС. О недостатках безопасности ОС HP-UX АИБ следует сообщать администратору ОС.

5. Обеспечить своевременное установления обновлений ОС.

6. Обеспечить периодическое тестирование ОС с помощью сканеров безопасности (например, ISS System Scanner).

4.1.3. Организационно-технические решения для защиты СУБД Oracle

1. С учетом того, что администратор СУБД имеет неограниченные права на управление содержимым журнала аудита, а действия администратора SYS вообще не регистрируются, необходимо исключить возможность неконтролируемого полного администрирования подсистемы аудита СУБД администратором базы данных путем:

– для администратора СУБД снять привилегии (Audit system, Audit any) работы с аудитом;

– создать дополнительную учетную запись администратора СУБД, предоставив ему только привилегии, необходимые для повседневной работы по управлению СУБД, при этом запрещая работу под именами *SYS* и *SYSTEM*, используя их только в случае чрезвычайных ситуаций;

– создать учетную запись АИБ и назначить ему права аудита. Поскольку в СУБД Oracle технически невозможно обеспечить эффективный контроль безопасности путем разделения на две половины административных паролей *SYS* и *INTERNAL* (например, пользователь-владелец данных uid:oracle автоматически имеет привилегии *INTERNAL*, роль *SYSDBA* имеет привилегии *SYS*), разделение паролей не выполняется и контроль осуществляется с помощью средств аудита СУБД, паролями *SYS* и *INTERNAL* владеет администратор СУБД;

2. Включить и настроить аудит базы данных Oracle:

– включить аудит с помощью параметра AUDIT_TRAIL=OS. При этом данные аудита будут записаны в файл аудита HPUX. Для обеспечения безопасной оперативной записи информации аудита на сервер аудита безопасности местоположение файла аудита назначается серверу аудита безопасности, который предоставляет свои файловые ресурсы через NFS. Местоположение файла аудита назначается путем установки переменной конфигурации Oracle AUDIT_FILE_DEST;

– сконфигурировать аудит следующих событий в СУБД Oracle:

а) всех неудачных SQL- команд;(AUDIT [SQL] BY SESSION WHILE NOT SUCCESS) - это одна запись протокола для каждого пользователя и объекта базы данных в каждом сеансе, независимо от количества событий.

б) операций администратора БД (AUDIT DBA BY SESSION). *Эта опция включает следующие операции аудита:*

– SYSTEM AUDIT – аудит команд NOAUDIT (отключение аудита);

– PUBLIC DATABASE LINK – создание и удаление публичных ссылок на объекты удаленных баз данных;

– PUBLIC SYNONYM – создание и удаление публичных синонимов (альтернативных имен) объектов БД;

– ROLE – создание, изменение, установку, удаление ролей БД;

– SYSTEM GRANT – присвоение и удаление системных привилегий или ролей пользователям, или ролям БД;

– USER – создание, изменение, удаление пользователей БД;

в) команд SQL (DELETE, ALTER, CREATE, DROP) длятаблицБД,

г) операций по изменению прав на процедуры БД (AUDIT GRANT PROCEDURE BY SESSION);

– с помощью механизма редактирования ролей обеспечить, чтобы администратор БД и АИБ имели необходимые и достаточные полномочия для выполнения своих функциональных обязанностей, запретив при этом АИБ вносить какие-либо изменения в настройки СУБД, а администратору БД – искажать журналы аудита, для чего передавать их *на сервер аудита службы безопасности*;

– удалить привилегии DELETE ANY TABLE и AUDIT SYSTEM у администратора базы данных. Привилегия AUDIT ANY должна быть выдана только АИБ БД;

– поскольку СУБД Oracle не обеспечивает аудит пользователей SYS и INTERNAL, эти идентификаторы следует использовать только в том случае, если невозможно выполнить необходимые операции с помощью идентификатора DBA.

3. Обеспечить оперативный анализ и периодическое архивирование аудиторской информации, а также определить порядок взаимодействия отделов по результатам ее анализа:

– для быстрого анализа и формирования отчетов по результатам аудита базы данных необходимо разработать инструмент импорта аудиторской информации в базу данных SQL и программное обеспечение для выборки из этой базы данных, а также для формирования отчетов по результатам реализации политики безопасности. До завершения разработки программного обеспечения анализ текущего аудита выполняется администратором IP вручную;

– по результатам ежедневного онлайн-аудита АИБ может получить необходимую информацию о работе СУБД Oracle от администратора СУБД, который, в свою очередь, обязан предоставить такую информацию и обосновать выполняемые в СУБД операции, отраженные в файлах аудита.

4. Обеспечить усиленную проверки подлинности пользователей СУБД. Для усиления аутентификации в СУБД Oracle необходимо использовать одну из следующих систем: SecurID, Kerberos или RADIUS, которые позволяет обеспечить:

– трехстороннюю аутентификацию пользователя, сервера СУБД и сервера аутентификации;

– периодическое изменение аутентификационной информации во время работы пользователя;

– управление режимом доступа пользователя к серверу БД (время доступа);

– криптографическая защита соединения между пользователем и сервером БД;

– возможность использования личных идентификаторов для идентификации и аутентификации пользователей в БД.

5. Для реализации расширенной технологии аутентификации необходимо настроить сервер БД и клиентские части Oracle на использование технологии *third-party authentication*. В руководстве администратора СУБД Oracle подробно описывается установка службы расширенной аутентификации. Kerberos также может использоваться в качестве системы усиленной аутентификации в СУБД Oracle, которая также поддерживается Oracle.

6. Оптимизировать набор услуг на серверах HP-UX. Ввести профили пользователей, ограничивающие количество одновременных соединений (сеансов), продолжительность сеанса, продолжительность неактивного состояния;

7. Контролировать сертифицированными СЗИ целостность программных компонентов и конфигурационных файлов СУБД, а именно:

– файлов системных настроек СУБД;

– всех исполняемых файлов и библиотек СУБД.

7. Периодически тестировать СУБД с помощью сканеров безопасности на предмет обнаружения уязвимостей в СУБД и выработки рекомендации по их устранению (например, Database Scanner от ISS).

8. Обеспечить оперативное уведомление администратора СУБД от поставщиков ОС о новых исправлениях в СУБД и своевременную установку обновлений СУБД с уведомлением АИБ.

9. Обеспечить оперативное уведомление администратора СУБД о существующих обновлениях СУБД с точки зрения безопасности и АИБ об установке обновлений СУБД.

4.1.4. Организационно-технические решения для защиты сервера БД

В качестве возможных мероприятий по ограничению потенциальных угроз со стороны администратора _DBA могут быть выполнены следующие действия:

– создать замкнутую программную среду на АРМ администратора приложений для предотвращения запуска с него клиентского приложения прикладного ПО;

– установить средств защиты от НСД (аутентификация пользователя) на АРМ пользователей «закрытого» контура ИС для предотвращения доступа администратора на эти АРМ;

– организовать виртуальные выделенные подсети, объединяющие АРМ групп пользователей «закрытого» контура с различными полномочиями, с целью запрета доступа к серверу БД неразрешенных АРМ.

4.1.5. Организационно-технические решения для защиты АРМ пользователей ИС

1. Использовать только сертифицированные СЗИ от НСД на каждом АРМ. Настройку СЗИ от НСД на каждом АРМ производить индивидуально,

с учётом задач, независимо от используемой ОС. Блокировать выполнение пользователем собственных задач, не разрешенных АИБ.

2. В минимальной конфигурации СЗИ от НСД на каждом АРМ должны обеспечивать:

– создание закрытой программной среды для каждого пользователя (позволяет запускать только указанный набор программ и/или процессов);

– идентификацию и аутентификацию пользователей, предоставление доступа к компьютерным ресурсам только путем ввода пароля с клавиатуры;

– контроль целостности программного обеспечения СЗИ от НСД до входа пользователя в операционную систему;

– контроль целостности файлов системного и прикладного ПО, расположенных локально;

– разграничение доступа к локальным каталогам и файлам АРМ, обеспечивающее защиту от модификации системного и прикладного ПО АРМ;

– регистрацию попыток доступа к наиболее важным объектам локальной файловой системы компьютера;

– блокирование работы пользователей в случае нарушения ограничений, введенных СЗИ от НСД.

3. Управление доступом пользователей АРМ должно основываться на стандартных механизмах идентификации, аутентификации и разграничения доступа к ресурсам, предоставляемых:

– BIOS АРМ;

–СЗИ от НСД;

– ОС Windows;

– сетевой ОС;

– СУБД Oracle;

– серверами SecurID или Kerberos и др.

4. Завершение работы пользователя АРМ должно сопровождаться освобождением всех используемых ресурсов (выход из системы).

5. Настройка СЗИ от НСД должна запрещать пользователю выполнение следующих действий (табл. 4.2).

Таблица 4.2

Запрет на действия пользователя АРМ

Запрет	Пояснения
Загрузка с внешних носителей	Запрещается загрузка компьютера с системной дискеты или с загрузочного CD–диска
Работа при нарушении целостности	При обнаружении факта нарушения целостности контролируемых файлов доступ пользователя к компьютеру блокируется
Работа при изъятии аппаратной поддержки	При обнаружении факта изъятия устройства аппаратной поддержки из компьютера доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран будет выведено предупреждающее сообщение, и

Запрет	Пояснения
	загрузка компьютера будет прервана
Работа при изменении конфигурации	При обнаружении факта изменения конфигурации компьютера доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран выводится предупреждающее сообщение, и загрузка компьютера прерывается
Доступа к портам	Пользователю запрещается обмен информацией через коммуникационные порты компьютера
Редактирования системного реестра	Пользователю запрещается изменять параметры системного реестра
Изменения настроек сети	Пользователю запрещено изменение параметров работы сетевой карточки, сетевых протоколов и других настроек «сетевого окружения» в операционной системе
Изменения параметров безопасности	Пользователю запрещен доступ к изменению политик безопасности.
Выполнения функций, не определенных технологическим процессом	Пользователю запрещено выполнять программное обеспечение, не используемое в технологическом процессе

4.2.Организационно-технические решения для защиты корпоративной МСС

4.2.1. Общие технические решения для корпоративной защиты МСС

1. Пользователи должны иметь доступ к сетевым серверам, выделенным в отдельный сегмент, через строго определенный набор протоколов связи и приложений с использованием прокси-механизмов.

2. Пользователи, внешние по отношению к сети, не должны иметь доступа к ресурсам корпоративной сети региона за исключением ресурсов демилитаризованных зон «открытого» контура ЛВС согласно строго определенному набору протоколов связи и приложений.

3. Удаленное администрирование систем безопасности в сети должно осуществляться с использованием шифрования трафика управления IP-уровнем или с использованием протоколов управления, поддерживающих шифрование данных (SNMP v3).

4. Управление активным сетевым оборудованием корпоративной сети должно контролироваться специалистами отдела информационной безопасности с использованием механизмов регулярного аудита сетевого оборудования. Подсистема аудита должна управляться подразделениями информационной безопасности.

5. Защита сети должна основываться на следующих решениях:

– магистральное шифрование сетевого трафика в сегменте региональной сети при передаче между «закрытыми» контурами ИС;

– построение системы защиты сетевого уровня с помощью виртуальных частных VPN-сетей при передаче трафика между «открытыми» контурами ИС;

– использование брандмауэров для разграничения ресурсов физических и виртуальных сетей подразделений ИС;

– применение средств фильтрации информации на прикладном уровне и прокси-систем наряду с пакетными фильтрами;

– создание сегментов ЛВС на основе оборудования структурированной кабельной системы, и обеспечение защиты физического уровня на этой основе;

– минимизация количества точек доступа к периметру «открытых» контуров ИЭ и их обязательный контроль;

– применение средств усиленной аутентификации пользователей и ресурсов корпоративной сети;

– применение систем обнаружения вторжений на сетевом, системном и прикладном уровнях;

– обеспечение удаленного администрирования и аудита всех компонентов системы безопасности, организация регистрации событий и подотчетность пользователей и администраторов.

5. Необходимо применять специальное антивирусное программное обеспечение ко всей почте, а также осуществлять автоматический антивирусный контроль ЛВС и почтовых серверов.

4.2.2. Технические решения для защиты корпоративной МСС на базе сканеров безопасности

Одним из важнейших элементов технологии IP-безопасности организации является периодическая оценка корпоративной сетевой безопасности. Одним из методов автоматизации процессов такой оценки является метод, построенный на технологии интеллектуальных программных агентов или сканеров безопасности. Они предназначены для сканирования известных уязвимостей сетевых служб и неверных параметров конфигурации ОС, приводящих к «отказу в обслуживании», выявления уязвимостей, специфичных для конкретной сетевой ОС, проверки надежности службы NFS, проверки служб удаленного доступа и т. д.

Сканеры безопасности включают в себя продукты семейства Internet Scanner и System Scanner от ISS [24]. Они управляются централизованно и обеспечивают тестирование и создание отчетов с консоли безопасности. Система System Scanner (S2) установлена на серверах и брандмауэрах. Консоль управления S2 - на АРМ администратора безопасности ИС, система Internet Scanner - на АРМ администратора безопасности ИС и настроена на проверку уязвимости серверов ИС, маршрутизаторов, брандмауэров, DNS-сервера и т. д. Тестирование безопасности системы должно выполняться

ежедневно при наименьшей загрузке протестированных ресурсов с экспортом результатов в базу данных аудита.

4.2.3. Технические решения для защиты корпоративной МСС на базе систем обнаружения вторжений

Сканеры безопасности позволяют оценить безопасность корпоративной сети. Однако они не обнаруживают проникновение злоумышленника в сеть, поэтому вторым необходимым элементом защиты сети является система быстрого обнаружения и реагирования на атаки *RealSecure* [24], которая позволяет обнаружить атаку на сетевой узел путем обнаружения статистических шаблонов сетевого трафика и сравнения их с масками, хранящимися в базе данных. *RealSecure* - это система мониторинга сетевого трафика в режиме реального времени. Основная задача, которую выполняет этот продукт, - своевременное обнаружение атак. Идея их идентификации проста: любая атака соответствует определенному сетевому трафику, поэтому ее анализ позволяет определить факт проведения атаки и зафиксировать «следы» злоумышленника. Поскольку анализ информационных потоков выполняется в реальном времени, время отклика АИБ на атаку или неисправность может быть минимизировано. Система *RealSecure* использует распределенную архитектуру и имеет два основных компонента *RealSecure Detector и RealSecure Manager.* Первый компонент отвечает за обнаружение атак и реагирование на них и состоит из двух модулей - *RealSecure Network Engine (RNE)* и *RealSecure System Agent (RSA).* Сетевой агент устанавливается в «открытом» сетевом сегменте и обнаруживает атаки, «прослушивая» трафик. Системный агент устанавливается на контролируемый узел и обнаруживает несанкционированные действия, выполняемые на этом узле. Компонент *RealSecure Manager* отвечает за конфигурирование и сбор информации с детектора *RealSecure.* Управлять компонентами системы *RealSecure* можно как с помощью централизованной консоли, так и при помощи дополнительного модуля, подключаемого к системам сетевого управления HP OpenView (RealSecure OpenView Manager).

Системы обнаружения вторжений (IDS) также отслеживают, регистрируют, анализируют и реагируют в режиме реального времени на попытки использования протоколов и служб, нарушающих политики безопасности. Эти системы делятся по методу анализа входной информации: на основе знания (сигнатуры) или на поведении субъекта (статистики). Классификация (таксономия) систем указанного класса может осуществляться по источникам информации, используемым для этих систем. Входная информация может быть записями аудита, системными загрузками или сетевыми пакетами. Термин «аудит» относится к информации, предоставляемой системой относительно ее внутренних действий и поведения. Существуют IDS сетевого уровня (прослушивание сети и анализ сетевых пакетов для обнаружения атак), системного уровня (мониторинг операционных систем для обнаружения признаков вторжения) и прикладного

уровня (мониторинг отдельных приложений). IDS может анализировать события двумя способами: сигнатурным или статистическим.

IDS сетевого уровня рассматриваются как эффективное средство сбора информации о событиях, происходящих в сети. Преимущества IDS сетевого уровня:

1. Он устанавливается только в наиболее важных точках сети для мониторинга всего входящего сетевого трафика и обычно состоит из нескольких однонаправленных пассивных хостов, которые перехватывают сетевой трафик в разных частях сети и сообщают об атаках на одну консоль управления. Работа хостов IDS практически не влияет на саму сеть.

2. Обнаружение сетевых атак типа «отказ в обслуживании» и «фрагментация пакетов». Анализ содержимого пакета данных позволяет выполнять поиск команд или конкретного синтаксиса, используемого в атаках.

3. Возможность анализировать «on-line» трафик, что не позволяет хакеру удалить следы своего присутствия.

4. Обнаружение и реагирование в реальном времени для сбора информации об атаке и злоумышленнике до завершения атаки.

5. Регистрация отраженных нападений или попыток подозрительных намерений нарушителя, что важно при оценке и совершенствовании политики безопасности.

6. Независимость от операционных систем, установленных в корпоративной сети.

К недостаткам сетевых IDS можно отнести невозможность анализа зашифрованной информации противника (шифрование делает невозможным анализ интенсивности потока пакетов). Кроме того, большинство сетевых IDS не сообщают, была ли атака успешной (они сообщают только, что она была начата). После обнаружения атаки администраторы должны вручную исследовать каждый атакованный узел, чтобы определить, имело ли место вторжение.

Сегодняшняя IDS на уровне приложений отслеживает события, происходящие в приложении, посредством очного аудита (securitylog или syslogd). Они обнаруживают атаки, анализируя файлы журнала приложения и сравнивая новые записи с известными сигнатурами атак. Имея прямой интерфейс с приложением и знание приложения, IDS прикладного уровня имеют гораздо больше возможностей найти подозрительную активность в приложении. При обнаружении атаки система посылает сигнал тревоги администратору или активизирует другие определенные механизмы ответа.

Преимущества IDS уровня приложения:

1. Возможность подтверждения успеха или неудачи атаки на основе отложенного анализа журналов, содержащих данные о событиях, которые действительно произошли, дополняя раннее предупреждение о начале атаки с помощью IDS сетевого уровня.

2. Возможность анализа расшифрованного входящего трафика, поскольку он имеет интерфейс с приложением и может дешифровать трафик.

Однако IDS прикладного уровня более уязвимы, чем IDS уровня хост-системы, и могут быть атакованы и отключены, поскольку они выполняются как приложения на хосте, что является их недостатком.

IDS системного уровня анализируют активность хоста, за которой они следят, и точно определяют, какой процесс или пользователь проявляет подозрительную активность в операционной системе. Система IDS системного уровня может централизованно управлять несколькими хостами и сообщать о атаках на одну консоль безопасности.

Главные преимущества.

1. Строгий контроль работы пользователя на узле, который обычно осуществляется только администратором сети (доступ к файлам, изменение прав доступа к файлам, попытки установки новых программ и/или попытки доступа к привилегированным службам), а также контроль за изменениями в ключевых системных или исполняемых файлах и т.д., что часто позволяет отслеживать несанкционированную деятельность вплоть до отдельного пользователя.

2. Распределение событий аудита по классам для упрощения конфигурации системы аудита;

3. Параметризация информации, собранной в соответствии с пользователем, классом, событием аудита, успешным/неуспешным вызовом системы;

4. Обнаружение атак, пропускающих IDS сетевого уровня (например, атак с самого атакуемого сервера).

5. Обнаруживайте и реагируйте на атаку практически в реальном времени, так как они получают прерывание от ОС, как только появляется новая запись журнала.

6. Не требуется дополнительного оборудования (установка отдельного узла IDS в сети), поскольку программное обеспечение IDS системного уровня устанавливается на существующую сетевую инфраструктуру, включая файловые серверы, веб-серверы и другие используемые ресурсы.

7. Позволяет масштабировать систему путем установки дополнительных агентов при расширении списка контролируемых сетевых узлов.

Недостатки.

1. Программные агенты обычно должны устанавливаться и поддерживаться на каждом контролируемом хосте.

2. Возможность атаки «отказ в обслуживании» путем переполнения файловой системы аудита.

3. Не удается обнаружить распределенную атаку на все узлы сети, так как она отслеживает только входящий сетевой трафик на своем узле.

4. Трудности обнаружения и отражения атак типа «отказ в обслуживании».

5. Использование вычислительных ресурсов хостов, которым они управляют. Высокое потребление системных ресурсов при необходимости детального мониторинга (производительность процессора, потребление локального диска и архивной памяти).

4.2.4. Организационно-технические решения для защиты сетевого оборудования

Для защиты сетевого оборудования необходимо выполнить следующие настройки и операции.

1. Конфигурировать активное оборудование ЛВС со встроенной защитой и обеспечить:

– авторизацию адресов системы оконечных устройств портами концентратора для доступа к этому порту только из конкретной системы оконечных устройств;

– автоматическое отключение порта при несанкционированном обнаружении адреса;

– режим работы портов концентратора, обеспечивающий прием пакетов, адресованных только конкретному подключенному АРМ;

2. В ЛВС на физическом и/или логическом уровнях обеспечить разделение контуров для разных функциональных целей (например, конфиденциальной информации, общего пользования и др.).

3. Выделить серверы ИС в отдельный сегмент ЛВС.

4. «демилитаризованные зоны» подключить непосредственно к компьютеру, который обеспечивает межсетевое экранирование и шифрование IP-пакетов при передаче трафика между «открытыми» контурами ИС;

5. Во внутренней «демилитаризованной зоне» разместить:

– сервер DNS, «заявляющий» внешним сетям некоторое, строго регламентируемое адресное пространство, используемое приложениями для взаимодействия внешних и внутренних абонентов сети;

– прочие сервера, доступ к которым должен быть обеспечен по незащищенным каналам удаленным пользователям.

6. Во внешней «демилитаризованной зоне» разместить серверы:

– доступа внешних абонентов;

– авторизации внешних абонентов.

7. Исключить возможность использования так называемых «опасных» сервисов (приложений) на серверах внешней «демилитаризованной зоны», что может дать потенциальному нарушителю возможность перенастроить систему, скомпрометировать ее и, опираясь на скомпрометированные ресурсы, атаковать корпоративную сеть.

8. Запретить внешний доступ к ресурсам, расположенным в «открытом» контуре ИС за пределами «демилитаризованных зон».

Размещение информационных ресурсов и услуг, доступных извне (из других сетей), кроме «демилитаризованных зон» в «открытом» контуре ИС должно быть запрещено.

9. Запретить доступ из «открытого» контура ИС в обход внешнего брандмауэра уровня приложений. Контролируемый доступ от одного «открытого» контура к другому должен осуществляться с фильтрацией трафика через VPN.

10. Организовать доступ к сегменту серверов «открытого» контура ИС только через брандмауэр прикладного уровня, чтобы защитить их от атак типа «отказ в обслуживании».

11. Настраивать фильтры на брандмауэрах с учетом принципа «все, что не разрешено, запрещено». Правила фильтрации должны блокировать внешние пакеты с исходными IP-адресами компьютеров «открытого» контура, а также пакеты с установленным битом маршрутизации.

12. Минимизировать количество служб, выполняемых на хостах, оставляя только необходимые службы.

13. Брандмауэры (межсетевые экраны) прикладного уровня должны скрывать от внешних сетевых пользователей структуру корпоративной сети (IP-адреса, доменные имена и т.д.). Эти брандмауэры должны определять, какие пользователи, от каких хостов, в направлении каких хостов, в какое время, какие сервисы можно использовать. Брандмауэры должны определять способ аутентификации каждого пользователя при доступе к службе и должны фильтровать Telnet, Rlogin, FTP, SMTP, POP3, HTTP, LP, Rsh, Finger, NNTP, Sql * Net и другие, а также поддерживать внешнюю авторизацию и учет на основе протоколов RADIUS/TACACS и интегрироваться в систему обнаружения вторжений.

14. Минимизировать количество портов маршрутизатора и межсетевого экрана, открытых для TCP-соединений, предотвращать прохождение через маршрутизаторы брандмауэры пакетов с маршрутизацией по источнику, а также пакетов с направленной широковещательной передачей.

15. Организовать оперативное распространение АИБ статистических данных об использовании услуг, попытках НДД и т.д.

16. Для администрирования оборудования использовать локальную консоль или протокол SMNP v.3 для шифрования управляющего трафика. Управление другим активным сетевым оборудованием ЛВС должно осуществляться с использованием аналогичных мер информационной безопасности, описанных выше.

17. Параметры аудита внешнего маршрутизатора должны включать аудит нарушений, правила фильтрации и другие ограничения, а также все команды пользователя на уровнях привилегий. Вся информация аудита должна автоматически отправляться на сервер аудита безопасности для дальнейшего анализа. Данные системного журнала также должны быть отправлены на сервер аудита безопасности.

4.2.5. Организационно-технические решения для организации защиты межсетевого взаимодействия

Одной из базовых задач построения защищенных корпоративных сетей является проблема защиты информации в процессе ее передачи *по открытым каналам связи*. Использование технологии защищенных виртуальных сетей VPN позволяет обеспечить криптозащиту информации при организации защищенных каналов связи или защищенных туннелей между «открытыми» контурами ЛВС взаимодействующих систем [18, 25 - 29]. VPN-агенты могут осуществлять функции шифрования/расшифрования, аутентификации, а также контроль целостности сообщения посредством электронной цифровой подписи (ЭЦП) или имитовставки (ИВ).

Как правило, VPN-агенты поддерживают несколько стандартных протоколов организации защищённых туннелей, которые могут применяться на разных уровнях логической структуры эталонной модели архитектуры ВОС. Хотя эти протоколы могут находиться на всех уровнях эталонной модели, средства VPN являются только теми, которые полностью прозрачны для сетевых служб и приложений пользователя. Это протоколы защищенных туннелей канального, сетевого и транспортного уровней. Эти три уровня, которые в терминах модели ВОС образуют логическую структуру транспортной системы зоны взаимодействия открытых систем, также называются уровнями VPN. Чем ниже уровень эталонной модели, на которой реализована защита, тем она прозрачнее для приложений и невидима для пользователей. Однако снижение этого уровня снижает количество реализуемых услуг по обеспечению безопасности и усложняет управление. Чем выше уровень безопасности по модели OSI, тем шире спектр услуг безопасности, тем надежнее контроль доступа и проще настроить систему безопасности. Однако в этом случае увеличивается зависимость от используемых протоколов обмена и приложений.

Существует два способа создания безопасных туннелей данных на уровне LAN и оконечных устройств [18].

Туннели уровня LAN обычно прозрачны для рабочих станций. В этом случае рабочие станции отправляют все сообщения в виде обычного текста. Кодер отбирает и кодирует пакеты, а декодер на противоположном конце канала декодирует сообщения и передает их сетевому серверу.

Шифрование на уровне целевой системы выполняется на рабочей станции или сервере. В незашифрованном виде пакеты вообще не передаются по сети. Существует два типа такой связи: «клиент-клиент» (кодер и декодер установлены на конечных системах, а незашифрованных пакетов вообще нет) и «клиент-сеть» (клиент взаимодействует с системой шифрования сетевого уровня).

Защита информации в процессе передачи по открытым каналам связи основана на выполнении следующих функций:

– аутентификация взаимодействующих сторон;

– криптографическое закрытие передаваемых данных;

– подтверждение подлинности и целостности доставленной информации;

– защита от повтора, задержки и удаления сообщений;

– защита от отрицания фактов отправления и приема сообщений.

Примечание 4.1. Выбор методов и средств защиты технологии виртуализации следует проводить с учетом требований [30].

4.2.5.1. Протоколы VPN канального уровня OSI

Протокол туннелирования точка-точка (PPTP) был разработан Microsoft при поддержке Ascend Communications, 3Com/Primary Access, ECI-Telematics и US Robotics для обеспечения стандартного протокола туннелирования точка-точка. PPTP не указывает конкретные методы аутентификации и шифрования.

Протокол L2F туннелирования (Layer-2 Forwarding), разработанный Cisco Systems при поддержке компаний Shiva и Northern Telecom, также соответствует канальному уровню модели OSI. В этом протоколе также не указаны конкретные методы аутентификации и шифрования. В отличие от PPTP, L2F позволяет использовать не только PPP, но и другие протоколы, например SLIP, для удаленного доступа к своему интернет-провайдеру. Интернет-провайдеры не должны настраивать адреса и проверять подлинность при создании безопасных каналов по глобальной сети. Кроме того, различные протоколы сетевого уровня могут использоваться для передачи данных через защищенный туннель, а не только через IP, как в PPTP. Протокол L2F стал компонентом операционной системы Cisco IOS и поддерживается на всех выпускаемых устройствах взаимодействия и удаленного доступа.

Протоколы PPTP и L2F были представлены на рассмотрение Целевой группы по проектированию Интернета (IETF), и в 1996 году соответствующие комитеты приняли решение объединить их. Результирующий протокол, включавший лучшие из PPTP и L2F, назывался Layer-2 Tunneling Protocol (L2TP). Поддерживается компаниями Cisco, Microsoft, 3Com, Ascend и многими другими производителями.

Гибридный протокол L2TP сочетает в себе лучшие функции вышеуказанных протоколов и добавляет новые функции. Протокол L2TP может поддерживать любые протоколы высокого уровня и обеспечивает управление потоком данных, удаленную аутентификацию пользователей, безопасную установку виртуальных соединений, а также позволяет открывать несколько туннелей между пользователями, каждый из которых администратор может выделить приложению. Как и предыдущие протоколы канального уровня, спецификация L2TP не описывает методы аутентификации и шифрования. Таким образом, протокол L2TP является расширением протокола PPP с помощью функций аутентификации удаленных пользователей, установления безопасного виртуального соединения и управления потоком данных. Протоколы CHAP/PAP или другие могут использоваться для аутентификации в корпоративной сети до начала сеанса PPP. Гарантированная доставка информации в сеансе

обеспечивается нумерацией защищенных кадров в соединении, восстановлением потерянных и искаженных кадров. Протокол L2TP предусматривает три этапа установления соединения: установление соединения с удаленным сервером LAN; Аутентификация пользователя; Конфигурирование безопасного туннеля.

Протоколы защищенных туннелей на канальном уровне не зависят от протоколов сетевого уровня модели OSI, над которыми работают локальные сети, входящие в состав виртуальных сетей. Они позволяют создавать безопасные каналы для связи между удаленными компьютерами и локальными сетями, работающими по разным протоколам сетевого уровня. Пакеты этих протоколов криптографически защищены и инкапсулируются в IP-пакеты Интернета, которые транспортируются к месту назначения, образуя безопасные виртуальные каналы. Многопротокольность – является основным преимуществом протоколов инкапсуляции канального уровня.

Однако формирование криптографически защищенных туннелей между «открытыми» контурами взаимодействующих систем на основе протоколов канального уровня приводит к трудностям конфигурирования и поддержки виртуальных каналов связи. Кроме того, в протоколах формирования безопасных туннелей на канальном уровне не указаны конкретные методы шифрования, аутентификации, проверки целостности каждого передаваемого пакета, а также средства управления ключами.

Из вышесказанного можно сделать вывод, что протоколы для создания безопасных виртуальных линий связи на канальном уровне лучше всего подходят для защиты связи при удаленном доступе к LAN.

4.2.5.2. Протоколы VPN сетевого уровня модели OSI

Спецификация, описывающая стандартные методы для всех компонентов и функций защищённых виртуальных сетей, представляет собой протокол Internet Protocol Security (IPsec), соответствующий сетевому уровню модели OSI и являющийся частью шестой версии протокола IP-IPv6. IPsec иногда еще называют протоколом туннелирования третьего уровня (Layer-3 Tunneling). IPsec предоставляет стандартные методы проверки подлинности пользователей или компьютеров при инициировании туннеля, стандартные методы шифрования конечных точек туннеля, создания и проверки цифровой подписи, а также стандартные методы обмена криптографическими ключами между конечными точками и управления ими. Этот гибкий стандарт предлагает несколько способов выполнения каждой задачи. Методы, выбранные для одной задачи, обычно не зависят от методов для других задач. Для функций аутентификации IPsec поддерживает цифровые сертификаты популярного стандарта X.509.

Туннель IPsec между двумя локальными сетями может поддерживать несколько отдельных каналов передачи данных, что приводит к тому, что этот тип приложения обладает преимуществом масштабирования по сравнению с технологией уровня 2. IPsec может использоваться совместно с

L2TP. Вместе эти два протокола обеспечивают наивысший уровень гибкости в защите виртуальных каналов. Дело в том, что спецификация IPsec ориентирована на IP и, таким образом, бесполезна для трафика любых других протоколов сетевого уровня. Протокол L2TP не зависит от транспортного уровня, который может быть использован в гетерогенных сетях.

Архитектура семейства протоколов IPsec (рис.4.2) включает в себя:

– протокол управления ключами (InternetSecurityAssociationKeyManagementProtocol, ISAKMP [RFC 2408] и протокол обмена ключевой информацией IKE (InternetKeyExchange) [RFC 2409];

– протокол аутентифицирующего заголовка (AuthenticationHeader, AH);

– протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP).

– домен интерпретации (DomainofInterpretation, DOI), который доопределяя структуру блоков данных и задавая правила именования информации, определяющей безопасность (политики безопасности, криптографические режимы и алгоритмы), связывает IKE с протоколом, защита которого обеспечивается.

Протокол обмена ключевой информацией IKE. Алгоритмическая независимость протоколов AH и ESP требует предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых взаимодействующими сторонами. Эту функцию на фазе установления соединения в современной архитектуре IPsec реализует протокол обмена ключевой информацией IKE (InternetKeyExchange) [RFC 2407, 2408, 2409]. Протокол IKE принято рассматривать как расширение ISAKMP [RFC 2408], основой которого он является, хотя отдельные идеи заимствованы у Oakley (TheOakleyKeyDeterminationProtocol [RFC 2412]) и SKEME (AVersatileSecureKeyExchangeMechanismforInternet).

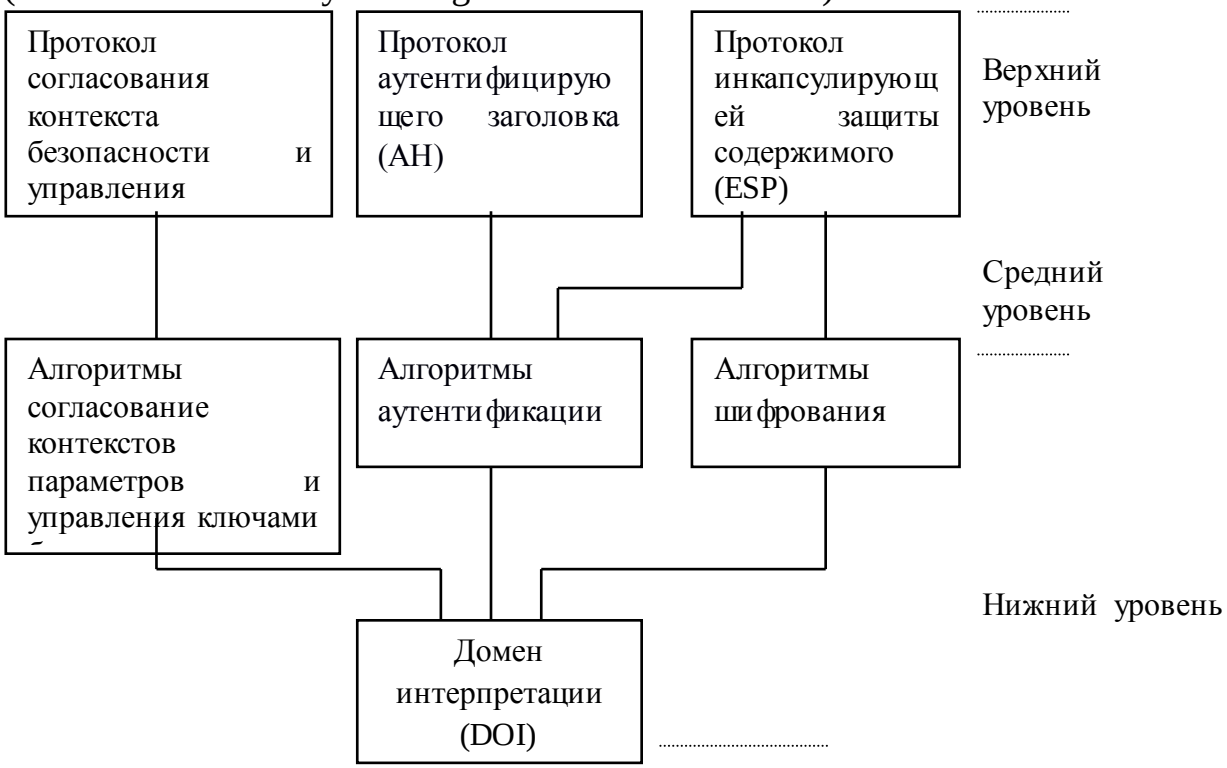

Рис.4.2. Архитектура семейства протоколов IPsec

Согласно протоколу IKE, при формировании безопасного виртуального туннеля взаимодействующие стороны должны разработать общий контекст безопасности (Security Association, SA) и только затем использовать элементы этого контекста [31]. Контекст безопасности SA для любого протокола представляет собой согласованный набор параметров, определяющих услуги и механизмы, предоставляемые этим протоколом для защиты трафика в сеансе связи, копия которого доступна каждой из сотрудничающих сторон. Контекст безопасности по существу представляет собой общее согласованное состояние отправителя и получателя, которое, в частности, определяет предоставляемые услуги, используемые криптографические алгоритмы и ключи в сеансе. Таким образом, основной целью IKE является автоматическое обеспечение безопасности согласования контекста безопасности для семейства протоколов IPsec между участниками мультимедийного сеанса.

В работе IKE можно выделить две основные фазы (phases). На первой фазе работы IKE происходит согласование обязательных параметров контекста безопасности IKE (IKESA), выполняется взаимная аутентификация участников, и устанавливаются сеансовые ключи. Контекст безопасности IKESA определяет, как именно будет обеспечиваться защита последующего трафика. Для семейства IPsec такими контекстами безопасности являются ESPSA и AHSA (общим названием этих контекстов безопасности является IPsecSA).

После завершения первой фазы и установления контекста безопасности IKE SA между инициатором и ответчиком любой из участников обмена может инициировать вторую фазу. На втором этапе фактически создается контекст безопасности IKE SA, который определяет способ защиты трафика в сеансе. Обязательные параметры IKE SA (алгоритм шифрования, алгоритм вычисления хэш-функции, метод аутентификации и группа Диффи-Хеллмана, определяющая параметры ключевого материала для обмена Диффи-Хеллманом) составляют защитный набор. На втором этапе могут выполняться обмены быстрым режимом, новым групповым режимом и информационным режимом. Основное различие между первой и второй фазами состоит в том, что конечные узлы IKE-соединения аутентифицируются в течение первой фазы, в то время как вторая фаза аутентифицируется для пользователей или приложений. После завершения первой фазы и установления контекста безопасности IKE SA между отправителем и получателем любой из участников обмена может инициировать вторую фазу. Во второй фазе могут выполняться обмены быстрого режима, режима новой группы, а также информационного режима. В ходе второй фазы согласуются, модифицируются и удаляются контексты

безопасности (которых может быть несколько) для протокола, использующего IKE.

Протокол аутентифицирующего заголовка AH и протокол инкапсулирующей защиты содержимого ESP. Как упоминалось выше, при формировании защищенного виртуального канала взаимодействующие стороны должны разработать общий контекст безопасности SA и только затем использовать элементы этого контекста, такие как алгоритмы и ключи. Для семейства IPsec такими контекстами безопасности являются ESP SA и AH SA (общее название этих контекстов безопасности - IPsec SA).

Протокол заголовка аутентификации AN обеспечивает аутентификацию источника данных, проверку его целостности и подлинности после приема, а также защиту от навязывания повторяющихся сообщений.

Протокол инкапсуляции содержимого ESP обеспечивает криптографическое закрытие пакетов передаваемых сообщений, а также выполняет все функции протокола AS. ESP может поддерживать функции шифрования и аутентификации/целостности в любой комбинации, то есть либо группу функций, только аутентификацию/целостность, либо только шифрование.

Протоколы AH и ESP не зависят от конкретных криптографических алгоритмов. Могут использоваться любые методы аутентификации, типы ключей (симметричные или несимметричные), алгоритмы шифрования и выделения ключей. Например, каждая страна может использовать свой собственный алгоритм, соответствующий национальным стандартам.

В настоящее время регистрируются два значения аутентификации для протоколов AS и ESP - HMAC-MD5 (Hashed Message Authentication Code - Message Digest версии 5) и HMAC-SHA1 (Hashed Message Authentication Code - Secure Hash Algorithm версии 1). Эти алгоритмы являются алгоритмами аутентификации секретного ключа. Если секретный ключ известен только передающей и принимающей сторонам, он обеспечивает аутентификацию источника данных, а также целостность пакетов, передаваемых между двумя сторонами. Алгоритм по умолчанию определяет алгоритм HMAC-MD5.

Для ESP зарегистрировано семь алгоритмов шифрования. Стандарт шифрования данных, как и алгоритм HMAC-MD5, является стандартом по умолчанию для совместимости с IPsec. В качестве альтернативы DES определены алгоритмы Triple DES, CAST-128, RC5, IDEA, Blowfish и ARCFour.

Протоколы AH и ESP поддерживают два режима:

а) туннельный режим. IP-пакеты защищены полностью, включая заголовки. Это главный режим. В этом режиме каждый обычный IP-пакет помещается полностью в криптографически защищенную форму в конверте IPsec, который, в свою очередь, инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуется на выделенных шлюзах безопасности, которые могут быть маршрутизаторами или брандмауэрами. Между этими шлюзами формируются безопасные туннели IPsec.

Туннелирование IP-пакетов полностью прозрачно для конечных пользователей. В оконечных системах туннельный режим может использоваться для поддержки удаленных и мобильных пользователей. В этом случае компьютеры этих пользователей должны иметь программное обеспечение, реализующее туннель IPsec. Протокол заголовка аутентификации AN [RFC1826], [RFC1827] обеспечивает аутентификацию источника данных, проверку его целостности и подлинности после приема и защиту от навязывания повторяющихся сообщений. В основе обеспечения целостности и аутентификации данных лежит шифрование с помощью односторонней функции (one-wayfunction), называемой также хэш-функцией (hashfunction);

б) транспортный режим. Только содержимое исходного IP-пакета помещается в конверт IPsec в криптографически защищенной форме, и исходный IP-заголовок добавляется к принятому конверту. Соответственно, в транспортном режиме заголовок IPsec помещается между заголовками сети (IP) и транспорта (TCP или UDP) обычного IP-пакета. Транспортный режим быстрее туннельного и предназначен для использования на терминальных системах. Это может использоваться для поддержки удаленных и мобильных пользователей и защиты информационных потоков в локальных сетях. В транспортном режиме IPsec помещает только содержимое защищаемого IP-пакета и добавляет исходный IP-заголовок к полученному конверту.

Заголовки блоков протоколов AN и ESP расположены в транспортном режиме после заголовка IP-пакета источника и перед заголовками протокола верхнего уровня, а в туннельном режиме - после заголовка внешнего IP-пакета и перед заголовком исходного IP-пакета (рис.4.3).

Транспортный режим	Туннельный режим
[IPисх.][AH][сервисный блок TCP/UDP]	[IPвнеш.][AH][IPисх.][сервисный блок TCP/UDP]
[IPисх][ESP][сервисный блок TCP/UDP]	[IPвнеш.][ESP][IPисх.][сервисный блок TCP/UDP]
[IPисх.][AH][ESP][сервисный блок TCP/UDP]	

Рис.4.3. Расположение полей заголовков протокольных блоков в транспортном и туннельном режимах

Сравнение различных режимов для протоколов AH и ESP представлено в табл. 4. 3.

Таблица 4.3.

Сравнение различных режимов для протоколов AH и ESP

Протокол	Транспортный режим	Туннельный режим
AH	Идентифицирует протокол-пассажир IP, а также отдельные части заголовка IP и заголовка расширений IPv6	Идентифицирует весь внутренний пакет IP (заголовок и протокол-пассажир внутреннего пакета IP), а также отдельные части внешнего заголовка IP и

		внешних заголовков расширений IPv6
ESP	Шифрует протокол-пассажир IP и все заголовки расширений IPv6, следующие за заголовком ESP	Шифрует внутренний пакет IP
ESP с аутентификацией	Шифрует протокол-пассажир IP и все заголовки расширений Ipv6, следующие за заголовком ESP. Идентифицирует протокол-пассажир IP и заголовок IP.	Шифрует внутренний пакет IP. Идентифицирует внутренний пакет IP.

Протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием, протокол AH должен применяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, в данном режиме допускается многократная вложенность туннелей с различными начальными и/или конечными точками. Поэтому в случае туннельного режима число возможных комбинаций по совместному использованию протоколов AH и ESP существенно больше.

4.2.5.3. Протоколы VPN сеансового уровень модели OSI

Безопасные виртуальные каналы также могут генерироваться на сеансовом уровне модели OSI. Для этого применяются так называемые «посредники каналов» (circuit proxy). Посредник работает над транспортным уровнем, шифрует и передает трафик из защищенной сети в общедоступный Интернет для каждого сокета по отдельности. При приеме выполняется обратная процедура. IP-сокет идентифицируется комбинацией TCP-соединения и определенного порта или указанного UDP-порта.

SSL/TLS (Secure Sockets Layer/Transport Layer Security), разработанный Netscape Communications, является наиболее популярным протоколом для шифрования на уровне сеанса. Этот протокол создает безопасный туннель между конечными точками виртуальной сети, обеспечивая взаимную аутентификацию абонентов, а также конфиденциальность, подлинность и целостность данных, циркулирующих через туннель. Ядром протокола SSL/TLS является технология комплексного использования асимметричных и симметричных криптосистем организации RSA Data Security.

Для стандартизации связи клиент-серверных приложений TCP/IP через сервер-посредник (брандмауэр) IETF утвердил протокол, называемый SOCKS. Пятая версия этого протокола (SOCKS5 [RFC1928]) используется для стандартизированной реализации канальных посредников в настоящее время. SOCKS5 поддерживает приложения, требующие контроля над направлениями информационных потоков и настройки условий доступа в зависимости от атрибутов пользователя и/или информации.

Согласно протоколу SOCKS5, клиентский компьютер устанавливает аутентифицированный сеанс с прокси-сервером. Использование этого прокси - единственный способ взаимодействия через брандмауэр. Посредник, в свою очередь, проводит любые операции, запрошенные клиентом. Поскольку брокер знает о трафике на уровне сеанса (сокета), он может осуществлять тщательный контроль, например, блокировать конкретные пользовательские приложения, если у них нет необходимых полномочий.

В отличие от виртуальных сетей, защищенных на сеансовом уровне модели OSI, виртуальные сети, защищенные на уровне канала или сетевом уровне, обычно просто открывают или закрывают канал для всего трафика в аутентифицированном туннеле. Это может быть проблемой, если ЛВС на другом конце туннеля не является надежной. Кроме того, установленные туннели канального и сетевого уровней работают одинаково в обоих направлениях, а защищенные сеансовым уровнем виртуальные сети обеспечивают независимое управление передачей в каждом направлении.

Виртуальные сети прокси-канала IPsec ориентированы на IP. Если IPsec по существу различает защищенные виртуальные каналы между различными парами взаимодействующих сторон, протокол SOCKS5 предоставляет защищенные туннели для каждого приложения и сеанса по отдельности. Аналогично протоколам туннелирования IPsec и канального уровня, виртуальные сети сеансового уровня могут использоваться с другими типами протоколов VPN, поскольку эти технологии не являются взаимоисключающими.

4.2.5.4. Распределение криптографических ключей и согласование параметров защищенных туннелей

При создании безопасных виртуальных сетей одной из наиболее важных функций является распределение криптографических ключей и согласование параметров безопасного туннеля. Эти функции выполняются при формировании каждого криптографически защищенного туннеля.

На уровне сети и сеанса модели OSI в большинстве случаев используются асимметричные криптосистемы, на основе протоколов распределения временных (сеансовых) ключей (SKIP, ISAKMP, SSL Handshake Protocol). При использовании этих криптосистем временные ключи распределяются с использованием главных открытых ключей. Распределение временных ключей на сетевом уровне чаще всего осуществляется алгоритмом Диффи-Хеллмана [32]. На уровне сеанса временные ключи обычно распределяются с использованием асимметричных систем, таких как RSA и El Gamal.

В протоколах формирования защищенных туннелей на канальном уровне модели OSI (PPTP, L2F, L2TP) временные ключи чаще всего генерируются на основе паролей пользователей [33]. Генерация осуществляется каждой стороной информационного взаимодействия после взаимной аутентификации. Согласование двух временных ключей,

генерируемых противоположными сторонами для одного защищаемого туннеля, обеспечивается их расчётом на основе одних и тех же параметров, включающих в себя согласованное случайное число или временную метку, а также хэш-функцию от пароля. Учитывая, что пароли являются аналогами основных ключей симметричного шифрования, более эффективным способом распределения временных ключей на канальном уровне является централизованное их распределение, например, на основе протокола Kerberos.

В зависимости от простоты реализации и достигаемой степени безопасности возможны следующие способы построения защищенного канала между двумя узлами компьютерной сети:

– для каждого соединения, устанавливаемого от имени какого-либо программного приложения;

– между сетевыми узлами и создание в рамках этого канала отдельных защищенных соединений, устанавливаемых от имени программных приложений;

Формирование защищенного виртуального канала для каждого соединения предполагает реализацию следующих этапов:

– выдача запроса одной из сторон и достижение соглашения на создание защищенного туннеля;

– аутентификация сторон, которая выполняется с помощью ранее распределенных основных ключей шифрования или назначенных паролей;

– распределение временных ключей и согласование параметров защищенного туннеля.

Вторая и третья фазы чаще всего пересекаются друг с другом, и аутентификация выполняется совместно с распределением временных ключей. Исключением является только случай проверки подлинности сторон осуществляемой на основе парольных методов.

В случае формирования между двумя сетевыми узлами общего защищенного канала, в контексте которого создаются отдельные защищенные соединения, перечисленные этапы выполняются также и при создании каждого защищенного соединения, устанавливаемого от имени программных приложений взаимодействующих сторон. Формирование между двумя сетевыми узлами общего защищенного канала и создание на его базе отдельных защищенных соединений характеризуется более высокой сложностью реализации. Однако в этом случае снижается уязвимость закрытых основных ключей, служащих для распределения главного сеансового ключа, и может быть обеспечено более эффективное расходование компьютерных ресурсов, затрачиваемых на генерацию временных ключей. Снижение ресурсных издержек на генерацию временных ключей достигается за счет переноса основной части вычислений на стадию распределения и генерации главного сеансового ключа.

4.2.3. Организационно-технические решения для организации защиты межсетевого взаимодействия с применением межсетевых экранов

Для межсетевой защиты в корпоративной сети и ее экранирования от атак извне, для обнаружения и регистрации внешних атак необходимо применение межсетевых экранов [13]. С помощью журналов аудита межсетевых экранов необходимо отслеживать:

– попытки соединения с ЛВС «открытого» контура с неразрешенных IP-адресов;

– попытки использования неразрешенных протоколов уровня TCP/UDP и соединения с неразрешенными портами серверов ЛВС «открытого» контура извне;

– попытки компрометации защищенных IP-соединений к ресурсам корпоративной сети;

– попытки использования незащищенных IP-соединений при межсетевом взаимодействии в региональной корпоративной сети.

Для оперативного анализа информации аудита необходимо настроить журнал syslogd межсетевых экранов таким образом, чтобы события аудита дублировались на сервер аудита службы безопасности, т. е. для всех межсетевых экранов хост loghost в файле /etc/hosts должен ссылаться на сервер аудита службы безопасности.

Для обеспечения надежности функционирования механизмов фильтрации трафика необходимо резервировать межсетевые экраны.

Известно [16], что любые механизмы защиты вносят временную, протокольную и потоковую избыточность в информационное окружение сети и приводят к ухудшению ее характеристик. Эти виды избыточности при проектировании защищенной корпоративной МСС должны быть учтены в ее критериях эффективности и ограничениях задач анализа [16]. Прикладные аспекты указанной проблемы связаны с повышением качества проектирования защищенных МСС, что в конечном итоге приводит к повышению эффективности использования сетевых ресурсов и сокращению затрат на их создание. В *Приложении 1* приведена формализация процессов предоставления механизмов защиты в корпоративной мультисервисной сети.

4.3. Организационно-технические решения по настройке журналов аудита на объектах мониторинга ИС

Система мониторинга ИБ ИС для выявления инцидентов ИБ постоянно осуществляет сбор и анализ событий журналов штатного аудита подконтрольных объектов ИС, в том числе СЗИ. При регистрации событий должны быть выполнены следующие требования:

1. Полнота регистрируемых событий должна быть достаточна и не избыточна для доказательного разбора ситуации;

2. Должна быть обеспечена максимально возможная независимость данных аудита от администратора контролируемой системы;

3. Должна быть обеспечена невозможность несанкционированного искажения журналов аудита, в том числе и администраторами контролируемой системы;

4. Хранение журналов аудита должно быть обеспечено в течение сроков, определенных руководящими документами ИБ организации.

Независимо от типа операционной системы в журналах штатного аудита должны регистрироваться следующие события:

1. Идентификационная информация, в том числе и попытки подбора пароля пользователями;

2. Операции, отвергнутые ИС из-за недостатка полномочий у пользователей;

3. Факты модификации конфигурационных файлов ИС;

4. Факты изменения администраторами полномочий пользователей «закрытого» и «открытого» контура ИС;

5. Факты отключения системы аудита администраторами;

6. Факты запуска и останова ИС.

4.3.1. Организационно-технические решения по настройке и сбору данных журнала аудита ОС HP-UX

Получение данных журнала аудита ОС HP-UX может осуществляться двумя способами:

1) на сервер, с консоли *«root»* инсталлируется агент, который в режиме «on-line» передаёт свой аудит. На серверной части обработки аудита, на основе двоичных событий аудита в формате ОС HP–UX формируются события для записи в базу данных сервера аудита службы безопасности. Достоинство данного режима заключается в следующем:

– агент осуществляет полностью автоматический режим управления подсистемой аудита (устанавливает для подсистемы аудита вспомогательный файл аудита, размер вспомогательного файла аудита, осуществляет сбор информации *из файлов wtmp, btmp, sulog* для генерации более качественных записей в БД, осуществляет контроль за размером *файлов wtmp, btmp, sulog*);

– ручная работа администраторов (пользователей *«root»* и *«auditor»*) минимальна, и сводится только к инсталляции агента и добавлению событий, подлежащих аудиту;

2) вторая схема предполагает накопление аудита на подконтрольных объектах и дальнейшее использование службы удаленного доступа к их файловым системам (например, по протоколу FTP) для переноса данных аудита на сервер аудита службы безопасности. После разбора, преобразования, аудит записывается в базу данных сервера аудита службы безопасности. Недостатки такого подхода заключаются в следующем:

– наличие ручной работы администраторов по управлению подсистемой аудита (установка вспомогательного файла аудита, размера файла);

– политика безопасности на серверах под управлением ОС HP-UX разрешает читать и записывать файлы аудита только пользователю *«root»*, это обеспечивается установкой прав доступа на файлы аудита (0600). Следовательно, для чтения данных аудита необходимо использовать учетную запись *«root»*;

– администратор должен как минимум раз в сутки переписывать заполненные файлы аудита с подконтрольных серверов на сервер аудита службы безопасности. Очевидно, что при большом потоке данных аудита съем аудита должен осуществляться чаще. Соотношение размера файлов аудита и периодичности их съема должны быть установлены в ходе опытной эксплуатации.

4.3.2. Организационно-технические решения по настройке и сбору данных журнала аудита СУБД Oracle

Требования к настройкам журнала штатной подсистемы регистрации событий.

Штатная процедура регистрации событий (ШПРС) СУБД Oracle опциональна. Опции аудита устанавливаются при помощи SQL-команды AUDIT. При эксплуатации с включенным аудитом требуется определенный расход вычислительных ресурсов СУБД, необходимый для генерации записей аудита. В случае неграмотной настройки аудита (например, включения аудита на применение всех привилегий ко всем объектам) может привести к полной неработоспособности СУБД из-за недостатка вычислительных ресурсов. Кроме того, при переполнении таблицы аудита, SQL-операции с БД, которые вызывают появление новых записей в таблице аудита, перестают выполняться. Поэтому необходимо точное определение перечня необходимых событий аудита и перечня объектов БД, для которых необходимо включить аудит.

В подсистеме аудита СУБД Oracle можно настроить аудит по следующим критериям:

– можно выполнять аудит конкретных SQL-операторов безотносительно к конкретным объектам. Например, можно генерировать запись аудита каждый раз, когда какой-либо пользователь выполняет оператор DROP TABLE, и не учитывать, к какой таблице относится этот оператор;

– можно выполнять аудит использования мощных системных привилегий. Например, генерировать запись аудита каждый раз, когда какой-либо пользователь применяет системную привилегию SELECT ANY TABLE для запроса к таблице БД;

– можно выполнять аудит определенных SQL-операторов для конкретных объектов БД. Например, генерировать запись аудита каждый раз, когда какой-либо пользователь удаляет запись из таблицы MODES;

– можно выполнять формирование одной аудиторской записи на применение каждого тип SQL-оператора в течение сеанса работы пользователя.

Наименее ресурсоемким и минимально необходимым является аудит привилегии CREATE SESSION, включение которого позволяет фиксировать факты регистрации и завершения работы пользователей. При наличии указанных фактов подсистема анализа способна выявить нетипичную активность пользователей:

– регистрация пользователя в СУБД в нерабочее время;

– регистрация с нетипичного для данного пользователя компьютера (терминала);

– регистрация пользователя в СУБД с именем, несоответствующим его имени в ОС.

С целью улучшения качества контроля, аудит для контролируемых объектов БД необходимо установить для всех пользователей СУБД. Для минимизации ресурсов, потребляемых аудитом, необходимо воспользоваться возможностью формирования одной аудиторской записи на каждый тип SQL-выражения.

СУБД Oracle генерирует записи аудита только после того, как аудит разрешен и для него установлены соответствующие опции. Например, можно установить опции аудита для конкретных субъектов. В Oracle разрешается сохранять генерируемые записи аудита либо в журнале аудита базы данных (фактически таблица записей аудита входит в состав контролируемой БД), либо в таком же журнале операционной системы, в которой работает СУБД Oracle Server. При использовании журнала аудита базы данных можно легко просматривать и находить записи аудита с помощью SQL-запросов и предварительно созданных для этого журнала представлений словаря данных.

4.3.3. Организационно-технические решения по настройке и сбору данных журнала аудита ОС Windows

Подсистема аудита ОС Windows обеспечивает регистрацию событий, связанных с работой ОС, и функционирование механизмов сохранения данных о событиях в журналы событий. В ОС Windows по умолчанию создаются следующие журналы событий:

– система (system);

– приложение (application);

– безопасность (security);

– установка (setup);

– перенаправленные события (forwarded events).

Системный журнал содержит события, записываемые системными компонентами ОС. Например, в журнале системы регистрируются сбои при загрузке драйвера или других системных компонентов в процессе загрузки системы. Типы событий, которые регистрируются компонентами системы, определены на уровне операционной системы.

В журнале приложений фиксируются события, относящиеся к работе приложений и программ. События, регистрируемые в журнале приложений, определяются разработчиками соответствующих приложений.

Журнал безопасности содержит события, связанные с безопасностью. Например, успешные и неуспешные попытки входа в систему, события, относящиеся к использованию ресурсов, такие как создание, открытие и удаление файлов и других объектов.

В журнале установки фиксируются события, связанные с установкой и обновлением системы, ее ролей, компонентов и приложений.

Журнал перенаправленных событий используется для хранения событий, собранных с удаленных компьютеров.

Состав событий, регистрируемых подсистемой аудита ОС Windows, определяется политикой аудита и настройками аудита конкретных объектов доступа (файлов, каталогов, ключей реестра, объектов каталога Active Directory и т. д.). Параметры политики аудита ОС Windows подконтрольных объектов необходимо настроить следующим образом:

– аудит входа в систему (audit logon events) – успех (success), отказ (failure);

– аудит изменения политики (audit policy change) – успех;

– аудит управления учетными записями (audit account management) – успех, отказ;

– аудит доступа к объектам (audit object access) – успех, отказ;

аудит доступа к службе каталогов (audit directory service access) – успех, отказ;

– аудит системных событий (audit system events) – успех;

– аудит отслеживания процессов (audit process tracking) – успех.

Для контроля функций управления локальными политиками подконтрольных объектов дополнительно необходимо настроить аудит доступа к соответствующим разделам реестра ОС, перечень которых приведен в табл. 4.4.

Таблица 4.4

Подконтрольные разделы реестра

Раздел реестра	**Описание**
HKLM\System\CurrentControlSet\Control\Lsa	Определяет дополнительные настройки штатной подсистемы аудита, настройки протокола сетевой аутентификации NTLM, параметры регистрации пользователей и сетевого доступа
HKLM\System\CurrentControlSet\Control\Print\ Providers\LanMan Print Services\Servers	Определяет настройки подключения принтеров
HKLM\System\CurrentControlSet\Control\ SecurePipeServers\Winreg	Определяет настройки удаленного доступа к реестру ОС

Раздел реестра	Описание
HKLM\System\CurrentControlSet\Control\Session Manager	Определяет настройки диспетчера сеансов
HKLM\System\CurrentControlSet\Services\ LanmanWorkstation	Определяет настройки клиента сети Microsoft
HKLM\System\CurrentControlSet\Services\LanManServer	Определяет настройки сервера сети Microsoft
HKLM\System\CurrentControlSet\Services\Netlogon	Определяет настройки сетевого доступа в домене
HKLM\System\CurrentControlSet\Services\LDAP	Определяет настройки клиента LDAP
HKLM\System\CurrentControlSet\Services\NTDS	Определяет настройки сервера LDAP
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Определяет настройки интерактивного входа в систему
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Setup\RecoveryConsole	Определяет настройки консоли восстановления
HKLM\Software\Policies HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies	Определяет множество параметров групповых политик для компьютера
HKLM\Software\Microsoft\Driver Signing	Определяет параметры проверки цифровой подписи драйверов устройств
HKCU\Software\Policies HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies	Определяет множество параметров групповых политик для пользователя

Аудит доступа к данным разделам реестра необходимо настроить следующим образом:

– задание значения (set value) – успех, отказ;

– создание подраздела (create subkey) – успех, отказ;

– удаление (delete) – успех, отказ.

Для всех разделов необходимо разрешить наследование прав аудита доступа вложенным разделам.

Для контроля функций управления групповыми политиками доменов дополнительно необходимо настроить аудит доступа на файлы шаблонов групповых политик (по умолчанию, расположены на контроллерах домена, в каталоге C:\Windows\SYSVOL).

Аудит доступа к файлам шаблонов групповых политик необходимо настроить следующим образом:

– создание файлов/запись данных (create files/write data) – успех, отказ;

– создание папок/дозапись данных (create folders/append data) – успех, отказ;

– удаление подпапок и файлов (delete subfolders and files) – успех, отказ;

– удаление (delete) – успех, отказ;

– смена разрешений (change permissions) – успех, отказ;

– смена владельца (take ownership) – успех, отказ.

Указанные настройки аудита следует разрешить наследовать вложенным подкаталогам и файлам.

Если регистрация событий вследствие настройки политики аудита вызывает значительное потребление ресурсов или быстрое переполнение файлов журнала, то нужно уменьшить состав регистрируемых событий за счет отказа от регистрации наиболее часто повторяющихся событий.

4.3.4. Организационно-технические решения по настройке данных журнала аудита СЗИ от НСД «Аккорд»

Программно-аппаратный комплекс СЗИ от НСД «Аккорд-Win32», «Аккорд-Win64» предназначен для применения на АРМ «закрытого» контура с ОС Windows для защиты информационных ресурсов от НСД при многопользовательском режиме эксплуатации [35].

СЗИ от НСД под управлением операционной системы и программного обеспечения ПЭВМ обеспечивает:

– защиту от несанкционированного доступа к ПЭВМ путем идентификации пользователей по не копируемым уникальным ТМ-идентификаторам DS 1992-1996 («Touch memory» - «Память касания») и их аутентификации по индивидуальному паролю, вводимому с клавиатуры. При этом обеспечивается защита от раскрытия индивидуального пароля пользователя;

– блокировку загрузки с отчуждаемых носителей (FDD, CD-ROM, ZIP Drive и др.) и прерывания контрольных процедур с клавиатуры;

– доверенную загрузку ОС и защиту от несанкционированных модификаций программ и данных;

– создание и поддержку изолированной программной среды, возможность реализации функционально замкнутых информационных систем на базе ПЭВМ;

– контроль целостности системных областей жестких дисков, программ и данных, а также конфигурации технических средств ПЭВМ до загрузки ОС;

– защиту от внедрения разрушающих программных воздействий: вирусов, закладок и т. д.;

– разграничение доступа пользователей к ресурсам ПЭВМ в соответствии с уровнем их полномочий;

– управление потоками информации на основе принципов дискреционного и мандатного доступа;

– регистрацию контролируемых событий, в том числе несанкционированных действий пользователей, в системном журнале, размещенном в энергонезависимой памяти контроллера комплекса. Доступ к журналу обеспечивается только АИБ;

– возможность подключения криптографических средств защиты информации.

СЗИ «Аккорд» сохраняет журналы ШПРС в виде файлов двоичного формата. Каталог, в котором сохраняются файлы, определяется настройками СЗИ «Аккорд» и хранится в ключе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Acrun, параметре LogsFolder. По умолчанию это каталог C:\ACCORD.NT или C:\ACCORD.X64, соответственно, для 32-х или 64-х разрядной версии ОС.

Имя файла в каталоге имеет вид ГГГГДДММЧЧММСС.LOW, где ГГГГДДММЧЧММСС – дата и время первой записи в данном файле. В одном файле журнала хранится информация об одном сеансе работы пользователя. Файл журнала имеет двоичный формат и состоит из заголовка и последовательности записей.

СЗИ «Аккорд» позволяет регистрировать события, представленные в табл. 4.5.

Таблица 4.5

Список событий журнала ШПРС СЗИ «Аккорд»

Мнемоническое описание	**Числовой код**	**Описание**
Событий класса «Реестр»		
LecoRegOpenKey	0	Открытие ключа реестра
LecoRegCloseKey	1	Закрытие ключа реестра
LecoRegCreateKey	2	Создание ключа реестра
LecoRegDeleteKey	3	Удаление ключа реестра
LecoRegEnumKey	4	Просмотр списка ключей реестра
LecoRegSetValue	5	Присвоение полю значение
LecoRegQueryValue	6	Просмотр значения поля
LecoRegDeleteValue	7	Удаление поля
LecoRegCreateValue	8	Создание поля
LecoRegEnumValue	9	Просмотр списка полей
События класса «Хранитель экрана»		
LecoSSOnAtTimeout	0	ScreenSaver включенповремени
LecoSSOnAtHotKey	1	ScreenSaver включен по горячим клавишам
LecoSSOnAtRemoute	2	ScreenSaver включен с АРМ АБИ
LecoSSOffAtTM	3	ScreenSaver выключен с помощью ТМ
LecoSSOffAtRemoute	4	ScreenSaver выключен с АРМ АБИ
LecoSSOffAtAdmin	5	ScreenSaver выключен с помощью ТМ администратора АРМ АБИ
LecoSSTimeDisable	6	Выключен временной контроль ScreenSaver-а
LecoSSTimeEnable	7	Включен временной контроль ScreenSaver-а
LecoSSOffBadTM	8	Попытка разблокировать не тем ТМ
События класса «Контроль файлов»		
LecoHStartCheck	1	Начало проверки списка файлов
LecoHEndCheck	2	Конец проверки списка файлов
LecoHStartUpdate	3	Начало обновления списка файлов
LecoHEndUpdate	4	Конец обновления списка файлов
LecoHTotalHash	5	Хэш списка файлов
LecoHTotalEDS	6	Подпись списка файлов
LecoHGetPrivateKey	7	Получение секретного ключа

LecoHFileCheck	8	Проверка файла
События «Отладочные сообщения СЗИ»		
LecoDebugString	0	Отладочное сообщение СЗИ
События для класса «Файловые операции»		
Leco21Terminate00	0	Прерывание программы
Leco21SetDate	0x2b	Установка даты
Leco21SetTime	0x2d	Установка времени
Leco21MakeDir	0x39	Создание каталога
Leco21RemakeDir	0x3a	Повторное создание каталога
Leco21ChangeDir	0x3b	Изменение каталога
Leco21CreateFile	0x3c	Создание файла
Leco21OpenFile	0x3d	Открытие файла
Leco21CloseFile	0x3e	Закрытие файла
Leco21DeleteFile	0x41	Удаление файла
Leco21GetSetFileAttr	0x43	Получение/установка атрибутов файла
Leco21Exec	0x4b	Запуск программы
Leco21Terminate	0x4c	Завершение программы
Leco21FindFirst	0x4e	Поиск файлов по маске (первый файл)
Leco21FindNext	0x4f	Поиск файлов по маске (последующие файлы)
Leco21RenameDir	0x50	Переименование каталога
Leco21RenameFile	0x56	Переименование файла
Leco21Traverse	0x6d	Не установлено

Требования к настройкам штатной подсистемы регистрации событий СЗИ от НСД «Аккорд».

1. Для каждого пользователя администратор может установить уровень детальности журнала ШПРС – низкая, средняя, высокая.

2. Для любого уровня детальности в журнале отражаются параметры регистрации пользователя, доступ к устройствам, запуск задач, попытки нарушения правил разграничения доступа, изменения правил разграничения доступа (в частности, изменение паролей).

3. Для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров – даты, времени и др.

4. Для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов.

5. Для целей системы достаточно среднего уровня детальности журнала. Если установка среднего уровня детальности журнала СЗИ от НСД «Аккорд» создает значительную нагрузку на системные ресурсы подконтрольного объекта, то допускается установка минимального уровня детальности журнала.

6. При установке прав доступа к журналам СЗИ от НСД «Аккорд» должны соблюдаться следующие правила:

– к файлам журнала должен быть доступ на чтение для всех учетных записей пользователей ОС;

– к каталогу, хранящему файлы журнала, должен быть доступ на просмотр содержимого.

7. При необходимости допускается изменить в настройках СЗИ каталог, в котором сохраняются файлы журналов. В этом случае следует выбрать каталог, доступный для чтения пользователю ОС Local System и не защищаемый СЗИ «Аккорд».

8. Поскольку система обладает собственными средствами регистрации событий, позволяющими выполнять мониторинг обращений к реестру и файловой системе, достаточно анализировать журнал ШПРС СЗИ от НСД «Аккорд» на предмет событий классов «Контроль файлов», «Хранитель экрана» и «Отладочные сообщения СЗИ».

4.3.5. Организационно-технические решения по настройке данных журнала аудита СЗИ от НСД Secret Net

Secret Net версий 6.x, 7.x – программный комплекс, сочетающий в себе большой набор функциональных возможностей по защите информации, средства централизованного управления настройками защитных механизмов, средства оперативного реагирования на действия внутренних злоумышленников и возможность мониторинга безопасности, защищаемой ИС [36]. СЗИ от НСД Secret Net может поставляться как в сетевом варианте исполнения, так и в автономном.

В сетевом вариантеSecret Net события ИБ фиксируют и клиенты, и сервер безопасности. При этом события сохраняются:

– в локальном журнале Secret Net;

– в централизованной БД сервера безопасности, функционирующей с использованием СУБД Oracle (для версий СЗИ от НСД Secret Net 6.x, 7.x). Для версии СЗИ от НСД Secret Net, начиная со сборки 7.2, БД сервера безопасности может функционировать с использованием СУБД Microsoft SQL Server.

К достоинствам эксплуатации сетевого варианта Secret Net относится:

– обеспечение централизованного управления настройками политики безопасности;

– интеграция с ОС Windows, расширяющая, дополняющая и усиливающая стандартные механизмы защиты;

– осуществление мониторинга и аудита политики безопасности в режиме реального времени;

– оперативное реагирование на события НСД;

– поддержка терминального режима работы пользователей с рабочей станцией;

– аппаратная идентификация пользователей;

– контроль целостности файлов;

– разграничение доступа к устройствам (CD\DVD, USB, Wi-Fi и т. д.).

В журнале аудита Secret Net используется такой же формат данных и состав полей записей, что и в журналах ШПРС ОС Windows. Загрузка записей для просмотра осуществляется только в программе просмотра журналов, поставляемой в составе Secret Net [36].

1.Настройка параметров аудита сетевого варианта Secret Net.

1. 1. Сервер безопасности имеет возможность централизованного сбора журналов ШПРС Secret Net с клиентских компьютеров в централизованную БД. Периодичность сбора устанавливается с помощью штатной утилиты Secret Net «Консоль управления» для каждого клиентского компьютера.

1.2. Параметры накопления аудита на клиентских компьютерах конфигурируются через групповую политику домен Secret Net. Для перехода к редактированию данных параметров необходимо на контроллере домена, перейти по главному меню Программы → Администрирование → Политика безопасности домена. Параметр «Максимальный размер журнала системы защиты» устанавливается в значение 50496 кбайт. Параметр «Политика перезаписи событий» устанавливается в значение «Затирать события по мере необходимости».

1.3. Для включения событий на регистрацию необходимо использовать ветку «Регистрация событий» редактирования групповой политики домена Secret Net. Минимальный набор событий, необходимый для регистрации средствами Secret Net:

– Вход/Выход (все события категории);

– Замкнутая программная среда (ЗПС): Запрет запуска программы;

– Замкнутая программная среда: Запрет загрузки библиотеки;

– Контроль целостности: Удаление учетной записи из задания ЗПС;

– Контроль целостности: Завершение обработки задания на контроль целостности;

– Централизованное управление КЦ-ЗПС: Добавление субъекта;

– Централизованное управление КЦ-ЗПС: Изменение субъекта;

– Централизованное управление КЦ-ЗПС: Удаление субъекта;

– Контроль конфигурации: Успешное завершение контроля аппаратной конфигурации;

– Разграничение доступа к устройствам: Подключение устройства;

– Разграничение доступа к устройствам: Отключение устройства;

– Разграничение доступа к устройствам: Запрет доступа к устройству.

Система имеет возможность также контроля работы механизмов защиты (шифрование файлов, полномочное управление, замкнутая программная среда и др.), а также пересылки журналов Secret Net с локальных компьютеров на сервер безопасности.

2. *Настройка параметров аудита локального варианта Secret Net*

2.1. Необходимо выполнить аналогичные описанным выше настройки в локальной оснастке на каждом компьютере с установленной СЗИ от НСД Secret Net. Для автоматизированного получения событий из локальной БД Secret Net, администратору СЗИ от НСД необходимо выполнить экспорт

событий из защищенной базы Secret Net в файл БД формата Microsoft Access на каждом компьютере с установленным Secret Net.

2.2. Для выполнения экспорта, необходимо с полномочиями локального администратора ОС запустить штатную утилиту Secret Net ***Журналы*** и затем на левой панели утилиты следует выбрать журнал Secret Net, и далее пункт меню ***Secret Net → Экспорт***. В появившемся диалогов окне следует задать параметры файла для сохранения результатов экспорта.

2.3. Для чтения данных файл ****.mdb***, полученный в результате экспорта, должен быть перемещен на компьютер функционирования агента. Для доступа к файлу экспорта необходимо создать ODBC-псевдоним (с использованием 32-х разрядной версии редактора ODBC-псевдонимов и драйвера Microsoft Access) и связать его с полученным файлом.

СЗИ SecretNet регистрирует настроенные события сразу после своей установки. Система регистрации событий СЗИ SecretNet не может быть отключена. Ее можно только расширить, доведя уровень детализации аудита до максимального (как локальных событий, так и сетевых). Максимальный уровень детализации подразумевает регистрацию таких событий, как операции открытия файлов на чтение, на запись, запись в файлы и так далее. Кроме того, могут регистрироваться отдельные операции с выбранными файлами.

В качестве контролируемых объектов могут выделяется следующие группы ПО, расположенного на клиентском месте:

– состояние системы защиты SecretNet - по умолчанию контролируется целостность файлов СЗИ, доступ к этим файлам;

– исполняемые файлы АРМ (EXE, COM, DLL и так далее) - протоколируется операции открытия на чтение/запись этих файлов и запуск исполняемых файлов. Протоколируется загрузка DLL-модулей прикладными задачами. Может дополнительно контролироваться целостность файлов;

– конфигурационные файлы прикладного программного обеспечения и специально выбранные файлы - может контролироваться целостность конфигурационных файлов и протоколироваться операции по чтению/записи этих файлов;

– сетевые события - протоколируются регистрация пользователя в корпоративной сети, операции отображения сетевых устройств, доступ к сетевым файлам.

4.3.6. Организационно-технические решения по настройке данных журнала аудита аппаратно-программный комплекс шифрования «Континент»

Основным назначением аппаратно-программного комплекса шифрования(АПКШ) «Континент» является защита информации, в корпоративных сетях, использующих для передачи данных протоколы семейства TCP/IP v. 4, а также защита сегментов VPN от проникновения извне [37]. В состав АПКШ «Континент» входят следующие компоненты:

– криптографический шлюз (КШ) «Континент»;

– центр управления сетью (ЦУС) КШ;

– программу управления сетью КШ.

АПКШ «Континент» обеспечивает:

– шифрование и имитозащиту данных, передаваемых по открытым каналам связи между защищаемыми сегментами сети;

– защиту внутренних сегментов сети от несанкционированного доступа извне;

– скрытие внутренней структуры защищаемых сегментов сети;

– централизованное управление защитой сети.

События аудита регистрируются в журналах аудита в виде отдельных записей [38]. На АПКШ с установленным ЦУС формируются как журналы КШ, так и журналы ЦУС. События, происходящие на КШ, регистрируются в локальных журналах КШ. Для централизованного доступа к записям содержимое локальных журналов перемещается через ЦУС на хранение в БД на сервер БД АПКШ «Континент». В системном журнале регистрируются события, связанные с работой подсистем КШ и ЦУС, а также события, регистрируемые другими СЗИ (например, ПАК «Соболь»). Для каждого зарегистрированного события сохраняются время регистрации, описание события, категория и ряд дополнительных параметров.

В журнале НСД хранятся записи о зарегистрированных событиях, свидетельствующих о возможных угрозах безопасности. Каждая запись содержит информацию о количестве зарегистрированных событий в течение одной минуты, а также ряде дополнительных параметров. В журнал НСД также осуществляется запись событий, связанных с IP-пакетами, отброшенными пакетным фильтром или не соответствующих ни одному правилу фильтрации.

Требования к настройке подсистемы регистрации событий АПКШ «Континент» приводятся ниже.

1.Для обеспечения сохранности записей журналов и их своевременного получения администратор АПКШ «Континент» 3.6 может централизованно настраивать следующие параметры:

– параметры локальных журналов КШ;

– параметры передачи журналов ЦУС;

– расписание передачи журналов в БД;

– параметры очистки БД от устаревших записей журналов.

При настройке параметров локальных журналов КШ должен быть указан максимальный размер журналов и выполнен выбор регистрируемых IP-пакетов.

2. В программе управления ЦУС необходимо вызвать контекстное меню нужного КШ и активировать команду «Свойства», в появившемся диалоговом окне «Свойства криптошлюза» перейти на вкладку «Журналы».

3. В группе полей «Максимальные размеры журналов» для каждого журнала необходимо указать размер пространства на жестком диске КШ,

которое отводится для хранения записей. Размер пространства указывается в килобайтах.

4. Размер системного журнала и журнала НСД необходимо установить в значение 10240 Кб, а размер журнала сетевого трафика установить в значение 12288 Кб. Таким образом, суммарный размер пространства, отводящегося для хранения журналов, не превышает границу в 32 Мб, которая введена в силу конструктивных ограничений [38].

5. При настройке расписания передачи журналов из буфера ЦУС в централизованную БД, необходимо руководствоваться принципом минимизации потерь данных журналов вследствие превышения заданного размера. Рекомендуется настроить агента ЦУС и СД на получение журналов из буфера ЦУС на ежечасный интервал, что позволит снизить вероятность потерь из-за переполнения.

6. Для обеспечения высокой скорости доступа к централизованной БД рекомендуется хранить в БД записи за последние 7 дней. Таким образом, в параметрах для агента ЦУС рекомендуется установить срок устаревания записей для всех журналов 7 дней и время очистки записей в БД установить на понедельник 8 часов 55 минут утра.

7. Для обеспечения возможности чтения данных средствами системы, необходимо периодически выполнять экспорт событий из журналов в текстовые файлы. Исходя из приведенных выше настроек времени хранения событий, следует проводить сохранение записей журналов в файл еженедельно в понедельник в 9 часов утра, после момента времени, когда ЦУС удалит из БД записи старее последних 7 дней.

4.3.7. Организационно-технические решения по настройке данных журнала аудита комплекса антивирусной защитой Dr.Web Enterprise Suite Server

Антивирус Dr.Web 10 Enterprise Suite Server (ESS) предназначен для организации и управления надежной комплексной антивирусной защитой компьютеров локальной сети организации [30]. Dr.Web ESS решает следующие задачи:

– централизованная (без необходимости непосредственного доступа персонала) установка антивирусных пакетов на защищаемые компьютеры;

– централизованная настройка параметров антивирусных пакетов;

– централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах;

– мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах.

Программный комплекс Dr.Web ESS имеет архитектуру клиент-сервер. Его компоненты устанавливаются на компьютеры пользователей, администраторов и на компьютер, выполняющий функции антивирусного сервера, и обмениваются информацией, используя сетевые протоколы TCP/IP.

Dr.Web ESS позволяет сохранить за пользователем защищаемых компьютеров права на настройку и управление антивирусными пакетами данных компьютеров, а также гибко ограничить их, вплоть до полного запрета.

Требования к настройкам штатной подсистемы регистрации событий комплекса антивирусной защитой Dr.Web Enterprise Suite Server:

– выполнить интерактивный вход в центр управления антивирусной защитой комплекса Dr.Web ESS с использованием учетной записи, имеющей административные полномочия на сервере Dr.Web ESS;

– выбрать в верхней части экрана раздел «Администрирование», далее в левой части экрана выбрать пункт «Конфигурация Dr.Web Enterprise Server»;

– в правой части экрана необходимо открыть раздел конфигурирования «Статистические данные» и выбрать опции «Инфекции в БД», «Ошибки сканирования в БД»;

– перейти на вкладку «Безопасность» и установить опции «Аудит операций», «Аудит внутренних операций», «Аудит операций Web API». Сохранить настройки.

4.3.8. Организационно-технические решения по настройке данных журнала аудита продуктов антивирусной защиты Лаборатории Касперского

Основным назначением продуктов Лаборатории Касперского является антивирусная защита [40]. Продукты также обеспечивают защиту от спама, хакерских атак, программ-шпионов. Программные продукты Антивируса Касперского для Windows поставляются в вариантах для серверов и рабочих станций. Антивирус может применяться как на автономных компьютерах пользователей, так и в корпоративной сети предприятия. Продукты имеют возможность для централизованного конфигурирования, управления, мониторинга ИБ через дополнительное ПО – *Kaspersky Security Center.*

Вфункции Сервера администрирования входит:

– хранение структуры логической сети (сетевой конфигурации);

– хранение копии конфигурационной информации компьютеров логической сети;

– организация хранилищ дистрибутивов приложений «Лаборатории Касперского»;

– удаленная установка и деинсталляция приложений на компьютеры;

– обновление антивирусных баз и программных модулей;

– управление политиками и задачами на компьютерах логической сети;

– хранение информации о событиях, происходивших на компьютерах логической сети;

– формирование отчетов о работе приложений в логической сети;

– распространение лицензионных ключей на компьютеры логической сети, хранении информации о лицензионных ключах;

– отправка событий от функционирующих на компьютерах логической сети задач. Такие события могут сообщать, например, об обнаружении на компьютере вирусов.

Подключение клиентского компьютера к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском компьютере. При подключении клиентского компьютера к Серверу администрирования выполняются следующие операции:

– автоматическая синхронизация данных:

– синхронизация списка программ, установленных на клиентском компьютере;

– синхронизация политик, параметров программ, задач и параметров задач;

– получение Сервером администрирования текущей информации о состоянии программ, выполнении задач и статистики работы программ;

– доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Имеется возможность вручную задать интервал между соединениями. Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Регистрация событий. В процессе работы Антивирус Касперского фиксирует различного рода события в свой журнал. Они могут быть информационного характера, а также нести важную информацию. Например, событие может уведомлять об успешно выполненном обновлении приложения, фиксировать ошибку в работе некоторого компонента, обнаружение вируса. В Антивирусе Касперского имеется возможность воспользоваться сервисом уведомлений для доставки информации до эксплуатирующего персонала различными способами.

Перед инсталляцией сервера администрирования инсталлируется СУБД. По умолчанию при инсталляции Kaspersky Security Center выполняется установка Microsoft SQL Express 2005 или Microsoft SQL Express 2008 (в зависимости от версии устанавливаемого продукта).

В ходе последующей инсталляции сервера администрирования создается БД Kaspersky antivirus (KAV) для накопления событий антивируса.

Имеется возможность включить генерацию событий антивирусом, работающим без централизованного администрирования, а также антивирусом, использующим централизованный сбор событий. При централизованной схеме сбора событий в Антивирусе Касперского имеется возможность записи событий в БД KAV и дублирования их в системный журнал ОС (Event Log) на сервере администрирования. Экспериментально установлено, что информация о произошедших событиях, фиксируемая в БД KAV более полная, чем информация из журнала ОС.

При необходимости получения событий непосредственно на компьютере с установленным Антивирусом Касперского, нужно конфигурировать список событий для регистрации на каждом таком компьютере.

Требования к настройкам штатной подсистемы регистрации событий.

1.Если Антивирус Касперского работает без централизованного администрирования, имеется возможность включить генерацию событий антивирусом и указать способ регистрации событий. При невозможности воспользоваться централизованным сбором событий при помощи сервера администрирования Антивируса Касперского, необходимо настраивать локальный сбор событий на каждом компьютере. При этом необходимо сохранять регистрируемые события в журнале Event Log ОС Windows.

1.1. Для ***Kaspersky Endpoint Security 10*** настройка выполняется следующим образом.

Необходимо открыть главное окно программы, выбрать вкладку ***Настройка***, выбрать группу параметров ***Интерфейс***, в параметрах ***Уведомления*** нажать кнопку ***Настройка….***

1.2.В окне ***Уведомления*** для типов событий и отдельных событий антивируса указывается, каким образом уведомления будут доведены до пользователя (сохранять в локальном журнале, сохранять в журнале событий Windows, уведомлять на экране, уведомлять по почте). Для целей ЕСМИБ ТУ для регистрируемых событий установить ***Сохранять в журнале событий Windows.***

2. Для настройки Антивируса Касперского, использующего централизованный сбор событий, необходимо создать политики централизованного управления клиентскими антивирусами, сервером администрирования, агентом администрирования. Настройка централизованного управления с помощью ***Kaspersky Security Center*** выполняется следующим образом.

2.1. Для сервера администрирования и клиентских компьютеров необходимо создать или настроить существующую политику защиты и общих параметров программ. Для запуска мастера создания/редактирования политики необходимо запустить оснастку централизованного администрирования ***Kaspersky Security Center***, затем в левой панели в дереве выбрать узел ***Сервер администрирования <имя сервера> → Управляемые компьютеры***. При необходимости выбрать группу управляемых компьютеров. Открыть вкладку ***Политики.***

2.2. Для создания политику управления клиентскими компьютерами для группы администрирования выбрать ссылку ***Создать политику Kaspersky Endpoint Security*** и следовать указаниям мастера создания политики. При выполнении шагов настройки политики руководствоваться документами, принятыми в эксплуатирующем подразделении.

2.3. На шаге ***Интерфейс*** в группе ***Уведомления*** нажать кнопку ***Настройка….*** В окне ***Уведомления*** для типов событий и отдельных событий антивируса указывается, каким образом уведомления будут доведены до

пользователя (сохранять в локальном журнале, сохранять в журнале событий Windows, уведомлять на экране, уведомлять по почте).

Созданная политика применится на всех компьютерах под управлением ОС Windows, входящих в группу администрирования, для которой создавалась политика.

2.4. При создании политики для сервера администрирования на вкладке ***Политики*** выбрать ссылку ***Создать политику***, указать имя политики, выбрать программу для создания групповой политики ***Сервер администрированияKaspersky Security Center*** и следовать указаниям мастера создания политики. В последующих диалогах мастера необходимо набрать имя политики и выбрать ***Kaspersky Security Center*** как ПО, для которого настраивается политика. Необходимо выбрать количество событий, хранящихся в БД KAV сервера администрирования, исходя из аппаратной конфигурации компьютера, используемого для сервера администрирования. Рекомендуется указать значение 400000.

2.5. Для настройки уведомлений существующей политики необходимо выбрать политику для группы администрирования, в правой части окна выбрать ссылку ***Настроить уведомления***. В окне ***Свойства <название политики>*** выбрать группу параметров ***События***, в правой части окна выбрать одно или несколько событий, нажать кнопку ***Свойства*** и открывшемся окне задать способ регистрации событий и способ уведомления о событиях.

Рекомендуется для всех событий установить опцию ***На Сервере администрирования в течение (дней)***. Не рекомендуется устанавливать значение меньше 30 дней, так как это может привести к потере событий для анализа.

В заключение отметим, что применение рекомендованных штатных настроек оборудования и рекомендованных организационно-технических мер по защите информации только частично реализуют требования ПОЛИТИКА. Для построения СИБ ИС требуемого класса защищенности следует также провести дополнительный анализ и выбор сертифицированных программно-аппаратных СЗИ.

Более того, несмотря на то, что создание СИБ *сводит к минимуму ущерб организации*, надо всегда помнить, что *основным фактором обеспечения информационной безопасности в ИС остается «человеческий» фактор*. Поэтому в процессе эксплуатации СОИБ *особое внимание надо уделять постоянному обучению персонала с принципами политики информационной безопасности и использованию средств защиты информации в ИС.*

Контрольные вопросы по гл.4

1. Какие общие организационно-технические решения применяются для защиты компьютерных ресурсов серверов и АРМ?

2. Какие технические решения по защите от НСД компьютерных ресурсов применяются на уровне ОС HP-UX?

3. Какие технические решения по защите от НСД компьютерных ресурсов применяются на уровне сервера СУБД Oracle?

4. Какие организационно-технические решения по защите от НСД компьютерных ресурсов применяются на уровне сервера БД?

5. Какие технические решения по защите от НСД компьютерных ресурсов применяются на уровне АРМ пользователей ИС?

6. Какие общие технические решения по защите от НСД компьютерных ресурсов применяются на уровне корпоративной сети?

7. Какие технические решения для защиты корпоративной МСС на базе сканеров безопасности?

8. Какие технические решения для защиты корпоративной МСС на базе систем обнаружения вторжений?

9. Какие организационно-технические решения применяются для защиты сетевого оборудования?

10. Какие организационно-технические решения применяются для организации защиты межсетевого взаимодействия?

11. Какие протоколы формирования защищенного туннеля применяются на канальном уровне? Какие их основные функциональные достоинства и недостатки?

12. Какие протоколы образуют архитектуру защиты межсетевого уровня IPsec?

13. Какие работает протокол обмена ключевой информацией IKE?

14. Какие основные отличия работы протокола аутентифицирующего заголовка АН в транспортном и туннельном режиме?

15. Какие основные отличия работы протокола инкапсулирующей защиты содержимого ESP в транспортном и туннельном режиме?

16. Какие протоколы VPN применяются на сеансовом уровне модели OSI?

17. Как осуществляется распределение криптографических ключей и согласование параметров защищенных туннелей?

18. Какие организационно-технические решения применяются для организации защиты межсетевого взаимодействия с применением межсетевых экранов?

19. Какие общие организационно-технические решения по настройке штатных журналов аудита применяются на объектах мониторинга ИС?

20. Какие организационно-технические решения по настройке и сбору данных журнала аудита применяются для ОС HP-UX?

21. Какие организационно-технические решения по настройке и сбору данных журнала аудита применяются для СУБД Oracle?

22. Какие организационно-технические решения по настройке и сбору данных журнала аудита применяются для ОС Windows?

23. Какие организационно-технические решения по настройке данных журнала аудита применяются для СЗИ от НСД «Аккорд»?

24. Какие организационно-технические решения по настройке данных журнала аудита применяются для СЗИ от НСД SecretNet?

25. Какие организационно-технические решения по настройке данных журнала аудита применяются для аппаратно-программного комплекса шифрования «Континент»?

26. Какие организационно-технические решения по настройке данных журнала аудита комплекса антивирусной защитой Dr.Web Enterprise Suite Server?

27. Какие организационно-технические решения по настройке данных журнала аудита применяются для продуктов антивирусной защиты Лаборатории Касперского?

Глава 5. Построение системы управления информационной безопасностью информационной системы

Как было отмечено выше, информационная безопасность достигается проведением руководствомсоответствующего уровня *Политики организации.*Одноименный документ разрабатывается и принимается как официальныйруководящий документ, ведомством, организацией. ***Политика определяет, что нужно защищать.*** Поэтому после определения официальной политики безопасности следует определить конкретные меры и средства, реализующие практические процедуры защиты, соответствующие требованиям ПИБ. ***Процедуры безопасности определяют – как надо защищать ИС***, т. е. как именно необходимо выполнять требования политики безопасности. Таким образом, в организации должны быть разработаны не только политики безопасности, но и ясные процедуры безопасности, соответствующие политике.

Единый комплекс правовых норм, организационных мер, технических, программных икриптографических средств, обеспечивающий защищенность информации всоответствии с принятой политикойбезопасности ИС, образует ***систему информационной безопасности (СИБ) ИС.***Таким образом, СИБ – это совокупность защитных мер, средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, реализующая требования политики безопасности.

Для обеспечения контроля функционирования средств и механизмов защиты СИБ и эффективного их использования, а также для контроля состояния ИБ ИС в целом, предназначена ***система управления информационной безопасностью (СУИБ)***. СУИБ – часть менеджмента (руководства и управления) организации и предназначена для создания, эксплуатации, мониторинга, анализа, поддержки и совершенствования СИБ организации.

5.1. Принципы управления информационной безопасностью организации

5.1.1. Управление информационной безопасностью и международные стандарты

Управление информационной безопасностью (Information Security Management, ISM) – это управлениелюдьми,рисками, ресурсами, средствами защиты и т.п. Управление информационной безопасностью заключается в четкомвыполнениивсехпроцедурпообеспечениюИБ,координации и регулировании процедур, контроле их правильного, а такжеэффективноговыполнения.

Конечной целью создания СУИБ является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного) ИС.

Основной задачей системы является обеспечение необходимого уровня *доступности, целостности и конфиденциальности* компонентов (ресурсов) ИС. *Конфиденциальность* – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право. *Целостность* – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. *Доступность* – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

В мировой практике существуют разработанные модели систем управления ИБ, например, «Information Security Management Maturity Model» (ISM3, разработанная ISECOM), «The Systems Security Engineering Capability Maturity Model», стандарт NIST SP800–33.

Существует также ряд международных и национальных стандартов оценки ИБ и управления ею. Среди них: ISO/IEC 17799:2005 и первый стандарт новой серии ISO/IEC 27001, пришедший на смену английскому стандарту BS7799–2:2002, BSI. В отечественной практике первым в этой области стал стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС–1.0–2006, определяющий основные процессы СУИБ для организаций банковской сферы РФ; «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС-1.0-2014, общие положения; «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» РС БР ИББС-2.2-2009, методика оценки рисков нарушения информационной безопасности и др.

При построении СУИБ эксперты рекомендуют опираться на международные стандарты ISO 27001/17799. В этом случае, разработанная СУИБ позволяет достичь необходимого уровня защищенности системы и значительно снизить риск реализации угроз информационной безопасности. Однако прямое использование моделей и стандартов ISO/IEC 27001 и ISO/IEC 17799:2005 для построения СУИБ затруднительно. Либо они слишком конкретизированные, а в любой организации, как правило, уже существует определенная система процессов, ролей, организационно–распорядительных документов информационной безопасности, которые необходимо интегрировать в систему управления ИБ. При этом не определяются приоритеты, так называемые «веса директив», которые обычно применяются в стандартах аудита. Либо, напротив, рекомендации носят слишком общий характер. Например, стандарты содержат либо набор контрольных директив, либо общий подход к управлению ИБ, то есть определяют, что нужно сделать, но не определяют, как это сделать.

В этой связи при разработке СУИБ можно использовать также методические рекомендации ITIL (Information Technology Infrastructure Library, библиотека лучшего мирового опыта в области организации работы ИТ–службы), а также модели управления ИТ–ресурсами и ИТ–сервисами

Microsoft Operations Framework (MOF). Целесообразность использования рекомендаций по управлению ИТ–ресурсами и ИТ–услугами (и в первую очередь процессов управления инцидентами, изменениями) при построении СУИБ обусловлена тем, что процессы обеспечения информационной безопасности неразрывно связаны с процессами защиты, а значит, и управления информационными системами и должны быть тесно интегрированы с процессами управления ИТ. Библиотека ITIL содержит комплекс необходимых для построения СУИБ рекомендаций. Во–первых, в ITIL с определенной степенью детализации описан процесс управления безопасностью (Security Management). Во–вторых, предоставление ИТ–услуг, включая сервисы информационной безопасности, относится к ответственности служб информационных технологий и информационной безопасности. Методы эффективной организации деятельности ИТ–служб обобщены в библиотеке ITIL и многократно испытаны. Кроме того, организации предъявляют сегодня жесткие требования по качеству ИТ–услуг (в том числе и по информационной безопасности), обеспечивающих поддержку базовых бизнес–процессов. Обеспечение гарантированного качества ИТ–услуг — одна из основных задач процессов ITIL.

Важно, что для построения эффективной СУИБ, аналогично управлению ИТ–услугами, необходима четко действующая система оперативного управления изменениями. В ITIL эти задачи решены путем организации процессов управления изменениями (Change Management). В настоящее время библиотека ITIL стала фактически стандартом в области управления ИТ–услугами и вобрала в себя лучшие подходы и методики, обобщающие накопленный мировой опыт. представлены процессы эталонной модели ITIL. Согласно методологии ITIL, в обеспечении информационной безопасности участвуют практически все процессы эталонной модели ITIL.

Интеграция процесса управления безопасностью в систему процессов управления ИТ–ресурсами и ИТ–услугами и применение сервисно–ресурсного подхода при построении СУИБ (когда обеспечение ИБ рассматривается как сервис с определенным уровнем качества, предоставление которого обеспечивается определенными финансовыми, техническими, трудовыми ресурсами) дают целый ряд преимуществ. В частности, появляется возможность правильной расстановки приоритетов для решаемых задач ИБ, повышения эффективности расходования ресурсов и средств, выделяемых на управление безопасностью, и как следствие — повышение управляемости системы ИБ в целом. Вместе с тем, одних рекомендаций ITIL для построения полнофункциональной СУИБ недостаточно. Во–первых, необходимо поддержание жизнеспособности СУИБ во времени, обеспечение ее жизненного цикла. Необходимые для этого компоненты и свойства СУИБ («контрольные точки») приведены в используемом стандарте ISO 27001. Во–вторых, в ITIL не содержатся некоторые важные составляющие СУИБ, например, планирование

обеспечения непрерывности работы. Необходимо также и более глубокое определение процессов обеспечения ИБ и их взаимосвязей. Например, для обнаружения инцидентов необходимо вести мониторинг подсистем ИБ, который связан с процессом мониторинга ИТ–систем, системами Aasset Management и т. д. Для устранения инцидентов ИБ необходима организация процесса управления инцидентами ИБ. Для поддержания жизнеспособности СУИБ необходимы также регулярный внутренний аудит СИБ, что требует обучения сотрудников и, естественно, финансирования. Важными составляющими обеспечения информационной безопасности являются также процессы управления информационными рисками, информирования сотрудников о политике ИБ, правилах работы с конфиденциальной информацией и пр. Кроме того, необходимо наложение на модель процессов ролевой модели СУИБ, то есть определение владельцев процессов, ролей сотрудников, которые эксплуатируют подсистемы ИБ и отвечают за соответствующие сегменты системы. Тогда в случае инцидента ИБ, например, нарушения сетевой защиты, можно будет проследить его влияние на другие процессы и подсистемы ИБ, определить ответственных за устранение таких инцидентов, оценить экономические параметры (какой ущерб нанесен, какие средства понадобятся для предотвращения такого рода инцидентов и т. д.). Некоторые рекомендации по построению ролевой модели содержатся в документах Microsoft Service Management function.

5.1.2. Принципы построения архитектурных решений СУИБ

В качестве базиса для построения архитектурных решений СУИБ выбраны следующие основные общие принципы [41]:

– масштабируемость;

– иерархичность построения;

– функциональная полнота;

– методологическое единство функциональных спецификаций ИС на всех уровнях архитектуры СУИБ;

– открытость архитектуры;

– ориентация на использование открытых стандартов;

– использование преимущественно готовых решений;

– ориентация на процессные принципы организации системы эксплуатации;

– эволюционность и сохранение ранее сделанных инвестиций.

Кроме того, при разработке архитектуры СУИБ необходимо соблюдать следующие специфичные принципы.

1. *Централизация и специализация управления*. Структура СУИБ должна быть ориентирована на структуру основных бизнес процессов организации и структуру подконтрольных объектов СУИБ.

2. *Необходимость и достаточность контроля**. Ни один из информационных активов и элементов инфраструктуры ИС области действия СУИБ не должен оставаться без контроля.

**Под контролем подразумевается механизм периодического сбора информации об подконтрольном объекте, ее структурирования и интерпретации в согласованных терминах, а также построения истории эволюции свойств.*

3. *Безопасность и эффективность применения средств мониторинга ИБ.* Для подконтрольных объектов, которые не поддерживают стандартные протоколы (например, SMNPv.3), либо если на уровне стандартных протоколов не обеспечивается сбор нужных первичных сообщений ИБ (например, для приложений прикладного уровня) возможно применение специализированных средств мониторинга ИБ (программных агентов). Применение средств мониторинга ИБ не должно приводить к деградации работы подконтрольных объектов и нарушать их функциональные свойства. Эффективность средств мониторинга ИБ должна определяться не только способностью контролировать состояние ИБ подконтрольных объектов, но и безопасностью этого контроля для их работы.

4. *Консолидация мониторинга ИБ*. При создании элементов СУИБ необходимо, чтобы осуществлялась:

– консолидация обработки событий (все события мониторинга ИБ, получившие качественную оценку угрозы ИБ, должны проходить через единую систему обработки и анализа, что позволит поддержать единый временной контекст состояния ИБ организации);

– консолидация представления состояния (большое количество события мониторинга ИБ необходимо консолидировать в виде оценки обобщенного состояния ИБ организации, что повысит информированность пользователей об уровне угрозы ИБ и ответственность служб СУИБ при реализации соответствующих регламентов безопасности. Обобщенная оценка состояния ИБ должна предусматривать иерархичность предоставляемой информации о состоянии ИБ организации для различных уровней архитектуры СУИБ (первичное сообщение ИБ – сообщение мониторинга ИБ – коррелированное сообщение мониторинга ИБ).

5. *Унификация*. Принцип унификации должен распространяться на:

– применяемые средства администрирования для типовых СУИБ;

– способы сбора первичных сообщений ИБ от типовых контролируемых объектов ИС;

– применяемые критерии классификации и категорированию первичных событий ИБ;

– универсальный классификатор коррелированных событий мониторинга ИБ организации;

– способы оценки и представления состояния ИБ;

– типовые регламенты по обработке и реагированию на коррелированные события мониторинга ИБ в ИС;

– способы передачи данных между компонентами СУИБ.

6. *Непрерывность мониторинга ИБ.* Мониторинг состояния ИБ организации должен осуществляться непрерывно (постоянно).

7.*Разделение функций управления и администрирования СУИБ.* В СУИБ на уровне функциональных компонент должны быть разделены задачи управления ИБ и администрирования СУИБ (прежде всего, настройка, конфигурационное управление на уровне аппаратно–программных комплексов).

8.*Принцип сервисного подхода к управлению ИБ.* Требования к управлению и контролю СУИБ задаются процессами СУИБ. Для обеспечения обратной связи с процессами СУИБ должны быть определены спецификации структурированных сообщений мониторинга ИБ, которые описывают параметры/метрики штатного состояния ИБ.

5.1.3. Модель Демнинга (PDCA)

Стандарт ISO 27001 декларирует два основных принципауправления безопасностью.

1. *Процессный подход к управлению безопасностью*, который рассматривает управление как процесс (набор взаимосвязанных непрерывных действий), акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных для достижения целей.

2. *Применение модели Демнинга или модели PDCA* (Планируй, Plan — Выполняй, Do — Проверяй, Check — Действуй, Act) как основы для всех процедур (процессов) управления ИБ.

Стандарт ISO определяет *PDCA*–модель как основу функционирования всех процессов (процедур) СОИБ (рис.5.1).

Рис. 5. 1. Этапы жизненного цикла процедур PDCA–модели СУИБ организации

Для каждой процедуры системы управления информационной безопасностью определяются правила выполнения, необходимые ресурсы, график выполнения, процедуры контроля, критерии оценки эффективности. Различные процедуры СУИБ должны последовательно и непрерывно выполняться на следующих этапах модели PDCA:

–планирование процедур (*этап «ПЛАНИРОВАНИЕ»*);

– внедрение процедур (*этап «ВЫПОЛНЕНИЕ»*);

– проверка эффективности выполнения ИБ (*этап «ПРОВЕРКА»*);

– совершенствование процедур - внесение необходимых изменений в СИБ и СОИБ в целом (*этап «СОВЕРШЕНСТВОВАНИЕ»*).

Далее через определенный период времени требуется заново пересматривать цели и задачи выполнения процедур, то есть заново приступать к выполнению первого этапа модели PDCA.

Основная сложность при реализации жизненного цикла СУИБ заключается в проверке эффективности ее процедур. Для каждой процедуры необходимо разработать *критерии эффективности*, по которым будет проверяться ее эффективность. Такие критерии требуется разработать также и *для всей СУИБ в целом*. Критериями оценки эффективности СУИБ могут быть, например, изменение количества инцидентов ИБ, квалификация пользователей в области ИБ и пр.

Целью СУИБ является обеспечение снижения риска ИБ (ущерба) и поддержание его уровня до приемлемой руководством организации величины при осуществлении бизнес-процесса. Процессы управления рисками являются одними из основных процессов СУИБ и включают в себя

1) анализ рисков (идентификация ценных активов, оценка рисков – расчет ожидаемого ущерба);

2) обработка рисков (выбор метода управления рисками, подготовка плана мероприятий по снижению рисков с указанием контрмер, расчет эффективности выбранных контрмер по снижению рисков, определение ответственных и сроки реализации контрмер, контроль выполнения);

3) разработка требований к системе мониторинга ИБ и контроля защитных мер СОИБ;

4) внедрение контрмер и системы мониторинга ИБ;

5) организация процесса мониторинга эффективности ИБ (сбор и анализ событий ИБ и выявление инцидентов ИБ);

6) принятие мер по усовершенствованию ИБ организации.

Пункты 1-3 относятся к этапу «ПЛАНИРОВАНИЕ», п.4 – к этапу «ВЫПОЛНЕНИЕ», п.5 – к этапу «ПРОВЕРКА», п.6 – к этапу «СОВЕРШЕНСТВОВАНИЕ»

Рассмотрим более подробно этапы жизненного цикла процедур PDCA–модели СУИБ организации

5.2. Этап «ПЛАНИРОВАНИЕ» процедур СУИБ

Целью выполнения деятельности в рамках группы процессов «ПЛАНИРОВАНИЕ» является запуск «цикла» СУИБ путем определения первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе «СОВЕРШЕНСТВОВАНИЕ».

Выполнение деятельности на стадии «ПЛАНИРОВАНИЕ» заключается в определении/корректировке области действия СОИБ и предусматривает проведение следующих работ:

– планировании системы управления рисками (СУР) ИС организации;

– планировании системы мониторинга ИБ и контроля защитных мер СОИБ.

В состав работ по планированию системы управления рисками ИС организации на этапе «ПЛАНИРОВАНИЕ» входят

– *анализ рисков;*

– *обработка рисков*.

В состав работ по планированию системы мониторинга ИБ и контроля защитных мер СОИБ входят

– *планирование организационно-технических решений по мониторингу состояния информационной безопасности ИС и контролю защитных мер;*

– *планирование системы самооценки ИБ организации;*

– *планирование типовой программы аудита ИБ;*

– *планирование системы непрерывности бизнеса организации.*

5.2.1. Планирование СУР ИБ организации. Анализ рисков в ИС

В процессе анализа рисков проводятся следующие работы:

– *идентификация и определение ценности всех активовв рамках выбранной области деятельности;*

– *оценка защищенности ИС*;

– *оценка рисковдля возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов*.

5.2.1.1. Идентификация и определение ценности активов

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

– 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 организации, их квалификация и опыт;

– нематериальные ресурсы (репутация и имидж организации).

Следует определить, нарушение информационной безопасностикакихактивов может нанести ущерб организации. В этом случае актив будетсчитатьсяценным, и его необходимо будет учитывать при оценкеинформационныхрисков. Инвентаризация заключается в составлении перечня ценныхактивоворганизации. Как правило, данный процесс выполняют владельцыактивов.

В процессе категорирования активов необходимо оценить ихважность для бизнес-процессов организации или, другими словами, определить,какой ущерб понесет организация в случае нарушения информационнойбезопасностиактивов. Данный процесс вызывает наибольшую сложность, так как *ценностьактивовопределяетсянаосновеэкспертныхоценокихвладельцев (субъективные оценки)*.Впроцесседанного этапа часто проводятся обсуждения между консультантами поразработкесистемыуправленияивладельцамиактивов.Этопомогаетпоследним понять, каким образом следует определять ценность активов с точкизренияинформационной безопасности (как правило, процесс определениякритичности активов является для владельца новым и нетривиальным). Кроме этого,длявладельцев активов разрабатываются различные методики оценки активов. В частности, такие методики могут содержать конкретные критерии (актуальныедляданной организации), которые следует учитывать при оценке нарушения конфиденциальности, целостности и доступности, т. е. оценке ущерба,которыйпонесет организация при нарушении конфиденциальности, целостности илидоступностиактивов.

Оценку критичности активов можно выполнять в денежных единицах ивуровнях. Однако, учитывая тот факт, что для анализа информационныхрисковнеобходимы значения в денежных единицах, в случае оценки критичностиактивов в уровнях, следует определить оценку каждого уровня в деньгах.Например,длябазовойоценкирисковдостаточно3-уровневойшкалыоценкикритичности:низкий,среднийивысокийуровни.При выборе шкалы важно учитыватьследующее:

– чем меньше количество уровней, тем ниже точностьоценки;

– чем больше количество уровней, тем выше сложность оценки (сложно определить разницу между, скажем, 7-м и 8-м уровнем 10-уровневой шкалы).

Кроме этого, следует иметь в виду, что для расчетаинформационныхрисков достаточно примерных значений критичности активов: необязательнооценивать их с точностью до денежной единицы. Однако денежноевыражениекритичности все равнонеобходимо. Рассмотрим подробнее принципы оценки критичности каждогоуказанногоактива. Информационные активы (или виды информации) оцениваются сточки зрения нанесения организации ущерба от их раскрытия, модификацииилинедоступности в течение определенноговремени.

Программное обеспечение, материальные ресурсы и сервисыоцениваются, как правило, с точки зрения их доступности илиработоспособности,т. е. требуется определить, какой ущерб понесет организация принарушениифункционирования данных активов. Например, нарушение системыкондиционирования в течение трех суток приведет к отказу серверов организациикним будет нарушен доступ и вследствие этого организация понесет убытки.

Сотрудники организации с точки зрения конфиденциальности и целостности оцениваются, учитывая их доступ к информационным ресурсам с правами на чтение и на модификацию. Оценивается, какой ущерб понесет организации при отсутствии сотрудника в течение определенного периода времени. Здесь важно учесть опыт сотрудника, его квалификацию, выполнение им каких-либо специфических операций.

Репутация организации оценивается в связи с информационными ресурсами: какой ущерб репутации организации будет нанесен в случае нарушения безопасности информации организации.

Заметим, что процесс категорирования активов должен подчиняться четким документированным процедурам организации. 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.

5.2.1.2. Идентификация угроз и уязвимостей для идентифицированных активов

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 ИС, в которой обрабатываются активы и которые могут привести к реализации угроз. Угрозы и уязвимости рассматриваются только во взаимосвязи друг с другом, так как *инцидент ИБ– событие, указывающее на действительную, мнимую или вероятную реализацию угрозы*, возникает в случае появления комплементарной 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.

Понятно,чторазличныеугрозыиуязвимостиимеютразное значение (разный вес) для информационной системы. Следовательно, необходимо определить, какие угрозы и уязвимости наиболее актуальны,или, другими словами, определить *вероятностьреализации угрозы через уязвимость*. *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).

Оценка уязвимостей активов ИС, обусловленных слабостями их защиты, предполагает определение вероятности успешного осуществления угроз безопасности.

Угрозы и уязвимости, а также их вероятность определяются врезультатепроведения технологического аудита защищенности информационнойсистемыорганизации. Такой аудит может быть выполнен как специалистамиорганизации(так называемый, внутренний аудит), так и стороннимиконсультантами(внешнийаудит).

5.2.1.3. Оценка рисков для возможных случаев успешной реализации угроз информационной безопасности

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей. Величина риска определяется на основе стоимости актива, уровня угрозы и величины уязвимости. С их увеличением возрастает и величина риска. Оценка рисков состоит в том, чтобы выявить существующие риски и оценить их величину, т. е. дать им количественную оценку. Существуют различные методики измерения и оценки рисков, например, табличные, с помощью количественных шкал и др. [42, 43].

Классическая формула оценки информационного риска:

$$R = P(V) * D,$$

где R– информационный риск; D– величина возможного ущерба; P(V)– вероятность реализации определенной угрозы через некоторые уязвимости, которая может быть определена как относительная частота появления количества инцидентов ИБ в общем объеме наблюдений событий безопасности за достаточно большой период, либо определена субъективно на основе опыта пользователей как мера уверенности появления инцидентов

ИБ.

Разработка методики оценки риска – достаточно трудоемкая задача. Во-первых, такая методика должна всесторонне описывать информационную систему, ее ресурсы, угрозы и уязвимости. Задача заключается в том, чтобы построить максимально гибкую модель информационной системы, которую можно было бы настраивать в соответствии с реальной системой. Во-вторых, методика оценки рисков должна быть предельно прозрачна, чтобы владелец информации, использующий ее, мог адекватно оценить ее эффективность и применимость к своей конкретной системе.

На сегодняшний день существует два основных метода оценки рисков информационной безопасности, основанных на построении: *модели угроз и уязвимостей и модели информационных потоков*.

Метод оценки рисков, основанный на модели угроз и уязвимостей. С точки зрения базовых угроз информационной безопасности существует два режима работы алгоритма, реализующего этот метод:

– одна базовая угроза (суммарная);

– три базовые угрозы.

Исходные данные:

– ресурсы (сервер закрытого контура, сервер открытого контура, МЭ открытого контура, СКЗИ закрытого контура, однонаправленный шлюз, оборудование ЛВС закрытого контура, оборудование ЛВС открытого контура);

– критичность ресурса (величина ущерба);

– отделы, к которым относятся ресурсы (закрытого и открытого контура);

– угрозы, действующие на ресурсы;

– уязвимости, через которые реализуются угрозы;

– вероятность реализации угрозы через данную уязвимость (на основе полученной модели проводится анализ вероятности реализации угроз информационной безопасности на каждый ресурс);

– критичность реализации угрозы через данную уязвимость.

Приведем алгоритм расчета рисков *по угрозе информационной безопасности*.

1. На первом этапе рассчитывается уровень угрозы по уязвимости Th наоснове критичности и вероятности реализации угрозы через даннуюуязвимость. Уровень угрозы показывает, насколько критичным являетсявоздействиеданной угрозы на ресурс с учетом вероятности еереализации.
2. Для расчета уровня угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе, суммируются полученные уровни угроз через конкретные уязвимости (для режима с одной базовой угрозой и для режима с тремя базовыми угрозами).
3. Аналогично рассчитывается общий уровень угроз по ресурсу CThR

(учитывая все угрозы, действующие на ресурс).
4. Рассчитывается риск по ресурсу R.
5. Рассчитывается риск по информационной системе CR в целом.

Таким образом, в результате работы алгоритма пользователь системы получает оценки риска:

– по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;

– суммарно по всем угрозам для ресурса;

– по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;

– по всем угрозам для информационной системы.

Кроме того, указанный алгоритм позволяет пользователю оценить эффективность контрмеры, а также эффективность комплекса контрмер.

Оценка рисков информационной безопасности, основанная намодели информационных потоков. Оценка рисков информационной безопасности, основанная на модели информационных потоков, осуществляется на базе модели ИС организации. Данная модель позволяет оценить защищенность каждого вида информации. Алгоритм позволяет получить следующие данные:

– реестр ресурсов;

– значения риска для каждого ценного ресурса организации;

– значения риска для ресурсов после задания контрмер (остаточный риск);

– эффективность контрмер;

– рекомендации экспертов.

Для того чтобы построить модель ИС, необходимо проанализировать защищенность и архитектуру построения информационной системы. Специалист по ИБ, привлекая владельца (менеджера) информационной системы (используя вопросники, интервью, документацию, инструменты автоматического сканирования), должен подробно описать архитектуру сети:

– все аппаратные (компьютерные) ресурсы, на которых хранится ценная информация;

– сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);

– отделы, к которым относятся ресурсы;

– виды ценной информации;

– ущерб для каждого вида ценной информации по трем видам угроз;

– бизнес-процессы, в которых обрабатывается информация;

– пользователей (группы пользователей), имеющих доступ к ценной информации;

– класс группы пользователей;

– доступ группы пользователей к информации;

– характеристики этого доступа (вид и права);

– средства защиты информации;

– средства защиты рабочего места группы пользователей.

Исходя из введенных данных, можно построить полную модель информационной системы организации, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Приведем алгоритм анализа.

1. Составить структурную схему ИС на которой необходимо отобразить:

– все ресурсы (сервер, АРМ и т.д.);

– отделы, к которым относятся ресурсы;

– сетевые группы (локальные сети), физические связи ресурсов между собой и их подключения к Интернет;

– виды ценной информации, хранящейся на ресурсах;

– пользователей (группы пользователей), имеющих доступ к ценной (конфиденциальной) информации.

2. Описать в виде таблиц средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящемся на нем с указанием веса каждого средства

3. Описать в виде таблицы вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а также наличие соединения через VPN, количество человек в группе для каждого информационного потока

4. Указать наличие у пользователей выхода в Интернет

5. Указать ущерб организации от реализации угроз ИБ для каждого информационного потока

6. Рассчитать риски для каждого вида ценной информации, хранящейся в ИС по угрозе «нарушение конфиденциальности», «нарушение целостности» и «нарушение доступности».

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

Большинство инструментальных средств анализа рисков соответствуют требованиям международного стандарта ISO 177799, за основу которого взят британский стандарт BS 7799.

5.2.2. Планирование СУР ИБ организации. Обработка рисков

После вычисления оценки рисков необходимо провести обработку рисков, которая включает

– *выбор способа обработки рисков;*

– *подготовку плана обработки рисков или плана мероприятий по снижению рисков с указанием контрмер (административные, организационные, программно-технические);*

– *расчет эффективности выбранных контрмер по снижению рисков.*

5.2.2.1. Выбор способов обработки рисков

Выбор способа обработки рисков лежит в основе первого этапа обработки информационных рисков, в процессе которого определяются какие действия по отношению к рискам требуется выполнить в организации. Основные критерии обработки рисков:

– принятие рисков;
– уклонение от рисков;
– передача рисков;
– снижение рисков.

Принятие рисков осуществляется в том случае, если уровень рисковпризнается приемлемым, т. е. организация не считает целесообразнымприменятькакие-либо меры по отношению к этим рискам и готова понестиущерб.

Уклонение от рисков —полное устранение источникариска.

Передача рисков — перенесение ответственности за риск на третьилица(например, поставщика оборудования или страховую организацию) безустранения источникариска.

Снижение рисков — выбор и внедрение мер по снижениювероятностинанесенияущерба.

В процессе обработки рисков сначала *требуется определить, какие изнихтребуют дальнейшей обработки, а какие можно принять*. Как правило, эторешается с помощью оценки приемлемого уровня риска. Риски, равные илинижеприемлемого, можно принять. Очевидно, что для рисков, превышающихприемлемый уровень, требуется выбрать дальнейшие меры по обработке.Приемлемый уровень риска определяется руководством организации илиспециальнойгруппой, в которую входят руководители и главные финансистыорганизации.В случае, когда в организации наблюдается большой разброс значенийриска(какправило,этоможетвозникнуть,есликритичностьактивовбылаопределена в денежных единицах, а не уровнях), информационные рискиможноразбить на категории и определять приемлемый уровень для каждой из нихотдельно.Этовызванотем,чтоснижатьразличныезначениярисковдоодногозаданного значения не всегда целесообразно (часто для снижениявысокихрисков до заданного уровня необходимы неоправданно большиезатраты).

На сегодня один из наиболее распространенных – уменьшение риска путем принятия комплексной *системы контрмер*, включающей программно–технические и организационные меры защиты. Контрмеры могут снизить уровни рисков различными способами (уменьшая вероятность осуществления угроз ИБ; ликвидируя уязвимости или понижая их величину; уменьшая величину возможного ущерба; способствуя восстановлению ресурсов ИС, которым был нанесен ущерб; выявляя атаки и другие нарушения безопасности). Близким является подход, связанный с *уклонением от риска*. Наконец, в ряде случаев допустимо *принятие риска*. В этой ситуации важно

определиться со следующей дилеммой: что для предприятия выгоднее – бороться с рисками или же с их последствиями, решая оптимизационную задачу.

После того как *стратегия управления рисками*выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасностис подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

5.2.2.2. Подготовка плана обработки рисков

По результатам этапа *«Выбор способов принятия рисков»* составляется «*Отчет об обработке информационных рисков организации*», который подробно описывает методы обработки рисков. Кроме этого, составляется «*План снижения рисков*», где четко описываются *контрмеры 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.

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.

5.2.2.3. Расчет эффективности выбранных контрмер по снижению рисков

Расчет эффективности принятых контрмер, является мерой снижения рисков ИБ. В случае применения метода оценки рисков, основанного, например, на модели угроз и уязвимостей для расчета эффективности контрмер после их задания необходимо повторно пройтипоследовательно по всему алгоритму вычисления оценки риска и вычислить значение нового риска по ресурсу (R_{new}). Таким образом, мы получаем значение двух рисков – риска без учетаконтрмеры(R_{old}) и риск с учетом заданной контрмеры (R_{new}). Эффективность E введения контрмеры рассчитывается по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

Если эффективность контрмеры недостаточна, например, не соответствует величине приемлемого риска, то необходимо уточнить контрмеры и пройтипоследовательно по всему алгоритму еще раз.

5.2.3.Разработка требований к системе мониторинга ИБ и критерию оценки эффективности ИБ

Одной из основных функций СУИБ является *мониторинг ИБ. Мониторинг ИБ* – постоянное наблюдение за объектами и субъектами ИС, влияющими на состояние ее безопасности, а также сбор, анализ и обобщение результатов наблюдений. При этом главной задачей системы мониторинга ИБ является задача выявления и обработки инцидентов ИБ, количество которых служит мерой эффективности функционирования СОИБ.

5.2.3.1. Планирование организационно-технических требования по мониторингу состояния ИБ и контролю защитных мер СОИБ

Процесс мониторинга должен удовлетворять требованиям оперативности обнаружения несанкционированных действий и непрерывности сбора и анализа результатов наблюдения. Целями мониторинга являются:

– контроль за выполнением требований нормативных актов регуляторов по обеспечению безопасности информации и требований ПИБ ИС организации;

– выявление нештатных (в том числе злоумышленных) действий в ИС;

– выявление инцидентов ИБ (событий ИБ, требующих расследования).

Основной задачей мониторинга СУИБ является наблюдение в режиме реального времени за активными субъектами системы (пользователями, процессами и др.), сбор и анализ данных о функционировании этих субъектов, обобщение результатов анализа и формирование качественной и/или количественной оценки состояния ИБ, а также оценки функционирования системы в целом. При этом особое внимание должно быть уделено наблюдению за действиями в системе привилегированных пользователей. Итоговая оценка может содержать информацию о доступности информационных активов системы, об обнаружении деструктивных воздействий и др. Результат указанной оценки должен оформляться в виде сообщений «несанкционированное действие» (НСД) и/или «инцидент ИБ» и оперативно пересылаться администратору ИБ (АИБ) системы.

Существует два класса принципиально различных моделей мониторинга информационной безопасности: 1) модели, основанные на знаниях и 2) модели, основанные на обучении.

Модели, основанные на знаниях или сигнатурные модели, предполагают непрерывное наблюдение объекта защиты на предмет выявления в нем следов (признаков, сигнатур) некоторого наперед заданного множества атак и их блокировки по заранее назначенным правилам. Идея состоит в том, чтобы каким–либо образом задать характеристики злоумышленного поведения (это и называется сигнатурами), а затем отслеживать поток событий в поисках соответствия с предопределенными образцами. Таким образом, *под сигнатурным анализом* понимается анализ событий мониторинга, выделяемых в потоке регистрируемых данных, на соответствие заданным событийным цепочкам (сигнатурам), определяемым специально настраиваемыми правилами (шаблонами, фильтрами). Каждое из правил представляет собой цепочку первичных событий с определенными параметрами (контекстом события). Анализируемый поток первичных событий анализируется на предмет присутствия в нем заданных цепочек. Сигнатурный анализ производится в режиме реального времени. С правилами связаны обработчики событий, в которых производится анализ контекста на соответствие данному правилу и вырабатывается необходимая реакция, а именно, генерируется результирующее событие – сообщение о НСД или инциденте. Другими словами, методы сигнатурного анализа позволяют фиксировать факты конкретных нарушений, механизм которых заранее известен. Самой сложной проблемой для сигнатурного подхода является обнаружение ранее неизвестных атак. Модели указанного типа имеют множество разновидностей. Например, классические системы защиты информации от НСД, системы штатного аудита ОС и СУБД, – являются их частным случаем.

Модели, основанные на обучении, основываются на измерении отклонений наблюдаемого поведения субъекта (пользователей, приложений, аппаратуры) от его допустимого поведения. При этом допустимое («хорошее») поведение субъекта выявляется в процессе обучения системы контроля при его штатной работе. Одним из методов выявления аномальной активности является статистический метод.

Статистический анализ позволяет оценить соответствие текущего или апостериорного сеанса поведения легальных субъектов ИС априорному шаблону их поведения, построенному за определенные периоды времени. При статистической обработке анализируются все события, фиксируемые системой мониторинга, а не только сигнатурные цепочки заданных событий. При этом предполагается, что существуют статистические параметры наблюдаемой системы, неизменность которых отражает стабильность характера поведения ее субъектов. Количественные изменения этих параметров свидетельствует, либо об изменениях поведения субъектов (в том числе связанных с несанкционированными действиями), либо о действиях субъектов, направленных на дестабилизацию системы (изучение ее устойчивости, исследование недокументированных возможностей, обнаружение ошибок в администрировании и т. д.). Необходимо отметить,

что типичной ситуацией в ИС является невозможность с помощью правил безопасности ограничить нежелательные действия легального пользователя, не лишив его при этом необходимой функциональности. В этой связи применение статистических методов играет большую эвристическую роль в системе мониторинга ИС, позволяя, во-первых, выявлять нетипичные действия легальных субъектов и, во-вторых, проводить более детальный анализ и дополнительные расследования.

Два подхода – статистический и экспертный хорошо дополняют друг друга, т. к. статистический подход хорош там, где существует понятие типичного поведения субъекта (т. е. распределения измеряемых величин в нормальной ситуации остаются относительно стабильными), а экспертный подход плохо справляется с неизвестными атаками (равно как и с многочисленными вариациями известных атак).

Проведенный выше анализ моделей нарушителя и угроз позволяет сделать вывод, что основную опасность с точки зрения несанкционированного доступа к информации в ИС и ее возможного искажения представляют собой действия лица, имеющего (или получившего путем преодоления средств защиты) наибольшие привилегии в любой подсистеме ИС – привилегии администраторов баз данных, операционных систем и СУБД. При этом они могут скрыть свои деструктивные действия с помощью удаления полей штатных журналов аудита в силу наличия у них значительных полномочий с одной стороны, и невозможности обеспечения полного контроля их действий штатными средствами – с другой. Например, в силу архитектуры СУБД Oracle, администратор СУБД имеет неограниченные права по управлению содержимым журнала аудита, а действия администратора SYS вообще не регистрируются в системе.

В этой связи мы приходим к выводу о необходимости внедрения в СУИБ независимых средств мониторинга ИБ для контроля за действиями привилегированных пользователей, или так называемых доверенных средств мониторинга ИБ. Дополнительно, в случае, если в функциональной структуре ИС имеется собственная служба информационной безопасности, ПИБ должна содержать требования по разделению полномочий, а также реквизитов доступа (паролей) в подсистеме между администраторами сопровождения ИС и АИБ. Штатный аудит операционных систем, СУБД, БД и сетевого оборудования может быть использован, в том числе, и для контроля действий администраторов со стороны АИБ.

Система внешнего (независимого) мониторинга представляет собой специально разработанные программные средства, основу которых составляют программные агенты (сенсоры), функционирующие на уровне драйверов соответствующих операционных систем.

Необходимо отметить, что независимый мониторинг часто является единственным инструментом контроля привилегированных пользователей, а именно, в тех случаях, когда невозможно ограничить выполнение ими не санкционированных/деструктивных действий, не лишив их при этом

необходимой функциональности. Кроме того, для некоторых систем дополнительно все права по управлению штатным аудитом могут быть переданы независимому администратору.

Учитывая значительный объем данных аудита, поступающих от различных контролируемых подсистем ИС, а также многообразие требований политики безопасности, которые должны быть отслежены через эти данные, становится очевидной необходимость автоматизации процесса их анализа. При этом особое значение должно быть уделено построению *единых (универсальных) системинтегрального мониторингаИБ (ЕСМИБ)*, позволяющих выявлять в режиме реального времени подозрительные действия пользователей, в том числе распределенные атаки на систему защиты.

5.2.3.2. Планирование основных принципов построения ЕСМИБ

Основная задача системы интегрального мониторинга ИБ – оперативное получение и одновременная обработка данных от всех компонент контроля ИС (в т. ч. внешних систем защиты), их формализация и экспорт в СУБД ЕСМИБ с последующим оперативным анализом этих данных. Такой подход позволит определять и анализировать распределенные атаки на ИС, при реализации которых записи в одном из журналов систем аудита или внешней системы защиты может оказаться недостаточно для гарантированного определения атаки, а требуется согласованный интегральный анализ событий, зарегистрированных в нескольких журналах аудита. Кроме того, согласованный анализ событий аудита позволит избежать ложного детектирования несанкционированный событий, вызванных случайными сбоями или ошибками пользователей. Результатом разбора данных аудита является принятие решения о воздействии на технологический процесс ИС с целью ликвидации последствий выявленных нарушений и недопущения их в будущем, а также формирование численных оценок опасности выявленных событий безопасности.

К ЕСМИБ должны предъявляться следующие требования [44-46]:

– возможность интерпретации журналов аудита всех компонент ИС (ОС, СУБД, систем защиты информации (СЗИ), систем обнаружения вторжений (IDS) и др.);

– возможность многоуровневого построения ЕСМИБ с реализацией предварительной и окончательной обработки данных аудита на различных компонентах ЕСМИБ;

– наличие центральной SQL–базы данных ЕСМИБ, в которой накапливается информация аудита компонент ИС;

– возможность дистанционного управления интегральными настройками аудита различных компонентов ИС для контроля конкретного субъекта. Например, обеспечить возможность интегрального аудита конкретного пользователя, при котором одновременно получается и анализируется информация о действиях пользователя на АРМ ИС, в СУБД Oracle, в

корпоративной сети по IP- адресу пользователя (от межсетевых экранов, маршрутизаторов) и др.;

– возможность связывания событий аудита от различных компонентов ИС для определения совокупных действий конкретного пользователя ИС или групп пользователей (должна быть разработана база соответствия имен пользователей в различных компонентах ИС), а также IP адресов или групп IP-адресов;

– наличие экспертного языка анализа журналов и возможность задания правил действий в зависимости от результатов анализа журналов аудита и возможность выдачи рекомендаций по воздействию на технологический процесс в ИС;

– возможность дистанционного оповещения администратора безопасности о выявлении НСД и/или инцидента в соответствии с заданными правилами.

Особенностью системы должно быть то, что *реакция на события НСД и инциденты ИБ*, описанные с помощью правил экспертной системы ЕСМИБ напрямую не должны влиять на функционирование ИС, а носить характер рекомендаций администраторам информационной безопасности (АИБ), целесообразность выполнения которых зависит от их решений и не может автоматически нарушить функционирование ИС.

Применяемые организацией меры по обнаружению инцидентов ИБ и реагирование на них должны обеспечивать:

– обнаружение и регистрацию инцидентов ИБ;

– организацию реагирования на инциденты ИБ;

– организацию хранения и защиту информации об инцидентах ИБ;

– регистрацию событий нарушения ИБ, связанных с результатами обнаружения инцидентов ИБ и реагирования на них.

ЕСМИБ должна основываться на анализе действий субъектов (пользователя, администратора, несанкционированного пользователя или администратора, процесса), как потенциальных источников атак на объекты ИС.

Для проведения работ по анализу регистрационных журналов в ИС должна быть организована центральная консоль управления ЕСМИБ, куда должны передаваться данные от подсистем независимого и штатного аудита, контроля целостности, подсистем анализа защищенности ИС и др. На этой консоли должна отображаться текущая ситуация по состоянию информационной безопасности в ИС. С этой консоли, в результате анализа текущей ситуации, автоматически или вручную, вырабатываются управляющие команды. Центральная консоль физически может быть реализована в виде нескольких рабочих мест (с выделением, например, места АИБ СУБД, администратора безопасности Unix–систем и т. д.). Такой подход к построению ЕСМИБ позволит:

– комплексно анализировать распределенные атаки на ИС, обобщать результаты анализа и выявлять скоординированные атаки на разные участки

системы;

– организовать в режиме реального времени автоматизированную обработку, классификацию и индикацию регистрационной информации по мере ее поступления;

– оперативно осуществлять выработку необходимых решений по улучшению защиты контролируемой системы от несанкционированных воздействий, а также формировать в режиме реального времени рекомендации (в виде выявленных типов аварийных ситуаций) администрации ИС для необходимой реакции на технологический процесс;

– *формировать численные оценки опасности* регистрируемых событий;

– избежать ложного детектирования несанкционированных событий, вызванных случайными сбоями или ошибками пользователей;

– интегрировать дистанционное управление настройками аудита компонентов ИС.

Для оперативного анализа регистрационных журналов и выработки отчетов по результатам такого анализа необходимо разработать инструмент импорта информации аудита в центральную SQL–базу данных аудита, реализованную в составе ЕСМИБ, и программное обеспечение для работы с этой базой данных, обеспечивающее выборку интересующих сведений аудита и формирования отчетов по результатам выполнения политики безопасности.

Так как существует большое разнообразие наблюдаемых компонентов ИС, каждая из которых обладает особенностями сбора и представления информации, ЕСМИБ должна быть способна использовать следующие механизмы сбора данных аудита:

– удаленные запросы ЕСМИБ к штатным SQL–базам аудита систем, как например к базе аудита СУБД Oracle, которая является уже готовым набором таблиц базы данных SQL и нуждается лишь в небольшой в дополнительной формализации;

– использование централизованной базы штатного аудита распределенных систем. Например, система аудита маршрутизаторов Cisco TACACS+ уже имеет централизованную базу данных аудиторской информации всех своих компонентов и системе интегрального аудита имеет смысл организовать работу непосредственно с этой централизованной базой данных;

– использование агентов трансляции данных аудита непосредственно на контролируемых объектах (например, ОС Unix). При отсутствии баз данных аудита компонентов ИС для передачи в ЕСМИБ данных аудита должны быть *разработаны агенты трансляции аудиторской информации*, например, для ОС HP–UX, которая не обладает механизмами удаленного предоставления данных аудита на базе архитектуры «клиент–сервер».

Кроме того, на этапе планирования системы мониторинга СУИБ и контроля защитных мер должны быть разработаны следующие нормативно-методические документы и процедуры:

– типовые документы, регламентирующие процедуры мониторинга СУИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты.

– типовая система классификациии категорированияпервичных событий ИБ объектов области действия СУИБи инцидентов ИБ.

– типовые документы и процедуры расследования инцидентов ИБ с учетом нормативных актов ФСТЭК, а также внутренних документов организации в области ИБ, в том числе:

– процедуры обнаружения первичных событий мониторинга ИБ и формирования инцидентов ИБ;

– процедуры классификациии категорирования первичных событий мониторинга ИБ и инцидентов ИБ;

– процедуры анализа причин инцидентов ИБ;

– процедуры информирования об инцидентах ИБ и нарушениях конкретных требований Политики ИБ и требований нормативных документов;

– процедуры формирования интегральной оценки состояния ИБ организации;

– процедуры поддержания в актуальном состоянии централизованной базы данных инцидентов ИБ;

– процедуры настройки отображения результатов мониторинга ИБ.

– типовые документы по хранению информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

– типовой порядок действий работников организации при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях.

– типовые роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ.

– типовые документы, регламентирующих процедуры сбора и хранения информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию защитных мер.

– типовые документы, определяющих роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также пересмотром указанных процедур.

5.2.3.4. Планирование самооценки ИБ организации

Для оценки состояния ИБ защищаемых активов и выявления признаков деградации используемых защитных мер проводится также самооценка соответствия СИБ требованиям ПИБ силами сотрудников подразделения технической защиты информации.

Планирование системы самооценки ИБ организации должно предусматривает разработку типовых документов, регламентирующих порядок проведения самооценки ИБ организации.

5.2.3.5. Планирование типовой программы аудита ИБ

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ, установления степени выполнения в организации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения независимой организации о состоянии ИБ организации.

Планирование типовой программы аудитов ИБ должно включать разработку типовой программы аудитов ИБ, содержащую информацию, необходимую для планирования и организации аудита ИБ, анализа и совершенствования СОИБ.

5.2.3.6. Планирование работ по контролю и анализу СУИБ

Планирование работ по контролю и анализу СУИБ должно предусматривать

– разработку плана выполнения деятельности по контролю и анализу СУИБ. В частности, указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации;

– разработку ролей, связанных с подготовкой информации, необходимой для анализа СУИБ руководством организации;

– разработку типового перечня документов для руководства по анализу СУИБ.

5.2.3.7. Планирование непрерывности бизнеса организации

Планирование непрерывности бизнеса организации должно включать:

1. Разработку типового плана непрерывности бизнеса организации, регламентирующего вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в котором должны быть учтены, в том числе

– процедуры реагирования на инциденты ИБ и оценки результатов реагирования (при необходимости с участием внешних экспертов в области ИБ);

– процедуры оценки ущерба, нанесенного инцидентом ИБ;

– мероприятия, которые должны быть предприняты после выявления инцидента ИБ;

– условия активизации плана непрерывности бизнеса организации;

– процедуры восстановления непрерывности бизнеса;

– процедуры тестирования и проверки плана;

– обучение и повышение осведомленности работников организации;

– обязанности работников организации с указанием ответственных за выполнение каждого из положений плана.

2. Разработку типовых документов и процедур в рамках управления ИБ, в том числе:

– типового перечня документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа функционирования СУИБ:

– отчетов с результатами мониторинга СУИБ и контроля защитных мер, в том числе содержащие информацию по выявленным инцидентам ИБ;

– отчетов по результатам анализа функционирования СУИБ;

– отчетов по результатам аудита ИБ;

– отчетов по результатам самооценок ИБ;

– документов, содержащих информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СУИБ;

– отчетов о новых выявленных уязвимостях и угрозах ИБ;

– отчетов по устранению замечаний руководства по итогам предыдущего анализа функционирования СУИБ;

– аналитических записок об изменениях в нормативно-распорядительных или законодательных документах по ИБ, которые могли бы повлиять на организацию СУИБ организации, например, изменениях в законодательстве Российской Федерации;

– отчетов по выполнению утвержденных руководством мероприятий по обеспечению требуемого уровня ИБ, например, выполнение планов обработки рисков;

– отчетов, подтверждающих выполнение требований непрерывности бизнеса и его восстановления после прерывания;

– ежемесячных и ежеквартальных отчетов (справок) о проведенных мероприятиях по совершенствованию СУИБ.

– отчетов по совершенствованию СУИБ;

– отчетов по контролю исполнения текущих, оперативных, внеплановых и плановых задач, указанных в плане мероприятий на год, долгосрочных задач, поставленных в соответствии с решениями руководства организации;

– отчетов по результатам внутреннего контроля выполнения требований по обеспечению ИБ в подразделениях организации;

– отчетов по ведению единой БД и поддержанию в актуальном состоянии организационно–распорядительных и нормативно–методических документов по вопросам обеспечения ИБ;

– отчетов по ведению единой базы знаний по вопросам оказания методической помощи АИБ подразделений и АИБ систем, текущего и оперативного контроля выполнения организационных требований по ИБ в виде листов опроса (анкетирования);

– отчетов по управлению ключевыми системами, в том числе организации и проведению плановых и внеплановых смен ключевых документов СКЗИ.

5.3. Этап «РЕАЛИЗАЦИЯ» процедур СОИБ

Задача этапа «РЕАЛИЗАЦИЯ» заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СУИБ, определенных на этапе «ПЛАНИРОВАНИЕ» и/ или реализации решений, определенных на этапе «СОВЕРШЕНСТВОВАНИЕ» и не требующих выполнения деятельности по планированию соответствующих улучшений.

В рамках выполнения процессов этапа «РЕАЛИЗАЦИЯ» СОИБ предусматривается проведение следующих основных работ:

1.Внедрение системы управления рисками.

2. Внедрение системы управления инцидентами.

3. Внедрение системы интегрального мониторинга ИБ.

5. Внедрение системы «Анализ функционирования СОИБ».

6.Внедрение типовой системы «Обеспечение непрерывности бизнеса».

5.3.1. Внедрение системы управления рисками

Управление рисками — процесс циклический. По существу, последний этап — это оператор конца цикла, предписывающий вернуться к началу. Проведение оценки рисков и выбор контрмер, как было обозначено, проводится на этапе «ПЛАНИРОВАНИЕ», на этапе «ВНЕДРЕНИЕ» выбранные контрмеры внедряются в СИБ, далее на этапе «МОНИТОРИНГ» осуществляется контроль и оценка эффективности внедренных контрмер, которая служит основанием для переоценки рисков на этапе «СОВЕРШЕНСТВОВАНИЕ» и на этапе «ПЛАНИРОВАНИЕ» цикл завершается планированием корректировки контрмер, которые, в свою очередь, внедряются далее на этапе «ВНЕДРЕНИЕ».

Для эффективного управления ИБ, в т. ч. управления рисками ИБ, разработаны различные специальные методики и инструментальные средства на основе международных и национальных стандартов ISO 15408, ISO 17799, РС БР ИББС, BS 7799-2:2005, ISO 27001, ISO 13335, BSI, COBIT, NIST 80030, COSO, SAS , Software Tool, MethodWare, Risk Advisor, CRAMM, RiskWatch, COBRA, ГРИФ, АванГард и др. [7, 8, 42, 43, 47-55].

На отечественном рынке имеется ряд продуктов указанного класса позволяющие осуществить управление рисками ИС с учетом различного уровням зрелости организаций. Указанные методики управления рисками разработаны, как правило, на основе требований международного стандарта ISO 17799.

Приведем краткое описание некоторых отечественных и зарубежных *инструментальных средства управления информационными рисками* (с учетом возможности их адаптации и применения в отечественных условиях), возможности которых приведены в [42, 43, 55].

5.3.1.1. Внедрение количественных методик и инструментальных средств управления рисками

К наиболее востребованных в нашей стране классу количественных методик и инструментальных средств управления рисками из зарубежных продуктов относятся CRAMM, RiskWatch, RiskAdvisor, а также отечественная экспертная система «АванГард».

CRAMM. Управление рисками в методике CRAMM осуществляется в несколько этапов, на которых:

1) определяются границы исследуемой информационной системы организации, состав и структура ее основных информационных активов и транзакций;

2) идентифицируются активы, и определяется их стоимость;

3) идентифицируются и оцениваются угрозы и уязвимости информационных активов организации;

4) проводится анализа рисков, который позволяет получить качественные и количественные *оценки рисков(расчет ущерба)*. Для оценки возможного ущерба предлагается ряд способов обработки рисков;

5) поиск адекватных контрмер (*меры и средств уменьшения или уклонения от риска)*. На этом этапе CRAMM генерирует несколько вариантов контрмер, адекватных выявленным рискам и их уровням.

CRAMM имеет средства генерации ряда отчетов, необходимых при проведении аудита информационной безопасности в соответствии с требованиями стандарта BS 7799 (ISO 17799).

CRAMM – пример методики анализа рисков и управления рисками, в которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Указанная методика также может быть применима в отечественной практике, хотя требования по ИБ российских РД и зарубежных стандартов различаются. Недостаток метода CRAMM с позиции отечественного потребителя состоит также в сложности русификации и большом объеме выходных документов (сотни страниц).

Методика RiskWatch. В основе продукта RiskWatch положена методика анализа рисков, которая состоит из четырех этапов.

1)Этап определение предмета исследования. Используются шаблоны по типу ИС организации (коммерческая ИС, государственная ИС и т. д.). В шаблонах в соответствии с типом ИС надо выбрать из указанных перечней: категорию защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты.

2) Этап ввода данных. Описывающих конкретные характеристики системы (ресурсы, потери и классы инцидентов). С помощью опросного листа выявляются возможные уязвимости. Задается частота возникновения угроз, степень уязвимости и ценность ресурсов.

3) Этап количественной оценки риска (рассчитывается профиль рисков и выбираются контрмеры).

4) Этап генерации отчетов.

К достоинству RiskWatch можно отнести простота и масштабируемость применения, легкая адаптация к требованиям ИБ отечественных регуляторов.

RiskAdvisor (организация MethodWare). ПО RiskAdvisor позволяет идентифицировать риски и угрозы, а также определить ущерб по результату реализации угроз и предложить контрмеры.

По сравнению с CRAMM методика *RiskAdvisor*значительно проще в применении итребует существенно меньшей трудоемкости.

Экспертная система АванГард (Институт системного анализа РАН) [49]. Типовой пакет программ системы АванГард включает два программных продукта: «*АванГард-Анализ*» и «*АванГард-Контроль».* При этом ПО «АванГард-Анализ» решает задачи управления ИБ (анализ рисков, формулирование целей безопасности и требований политики безопасности), а ПО «АванГард-Контроль» - решает задачу контроля уровня защищенности ИС (определение уязвимых мест защиты, т.е. таких мест в ИС, где требования ИБ не выполняются).

Экспертная система АванГард может использоваться для построения корпоративных методик анализа и управления рисков с учетом требования ПИБ организации и РД по ИБ отечественных регуляторов.

Единой методики, по которой можно было бы определить количественную величину риска, на сегодняшний день не существует. Во-первых, это обусловлено отсутствием необходимого объема статистической информации о возможности возникновения какой-либо конкретной угрозы. Во-вторых, играет немаловажную роль тот факт, что определить величину стоимости конкретного информационного ресурса порой очень трудно. Например, владелец информационного ресурса легко может указать стоимость оборудования и носителей, однако назвать точную стоимость данных, находящихся на этом оборудовании и носителях, он фактически не в состоянии. Поэтому самой часто используемой является качественная оценка информационных рисков, главные задачи которой – это идентифицировать факторы риска, определить возможные уязвимые области риска и оценить воздействие каждого из видов. [55].

5.3.1.2. Внедрение качественных методик и инструментальных средств управления рисками

Качественные методики управления рисками используют оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). К методикам указанного класса относятся *методики COBRA, RA Software Tool, FRAP и OCTAVE т др.* Опишем кратко возможности наиболее востребованных у нас.

Методика управления рисками COBRA. Эта методика достаточно проста в применении, т. к. для оценки информационных рисков организации использует небольшое количество *тематических вопросников* (*check list's*). Ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков организации и рекомендациями по их управлению. При необходимости перечень учитываемых требований можно дополнить

различными требованиями отечественных нормативных документов по ИБ регуляторов и/или организации.

Методика и инструментальные средства управления рисками RA Software Tool. В состав *RA Software Tool* входит ряд программных модулей, обеспечивающих проведение оценки рисков в соответствии как с требованиями базового уровня, так и с более детальными спецификациями руководства по оценке рисков PD 3002 Британского института стандартов (BSI).

5.3.2. Внедрение системы управления инцидентами ИБ

Международный стандарт ISO 27001:2005 обращает особое внимание на необходимость внедрения процедуры управления инцидентами ИБ.

В общем случае инцидент ИБ определяется как событие (или совокупность событий), которое может скомпрометировать бизнес–процессы организации или угрожает ее информационной безопасности (ISO/IEC TR 18044:2004). Под процедурой управления инцидентами ИБ будем понимать своевременную реакцию на инциденты безопасности и устранение их последствий с целью эффективного функционирования бизнес-процессов. При реализации процессов управления инцидентами ИБ рекомендуется использовать ГОСТ Р ИСО/МЭК ТО 18044.

Внедрение процесса управления инцидентам ИБ позволяет оценить эффективность функционирования СУИБ в целом и системы управления рисками, в частности. Частота появления и количество инцидентов ИБ, зафиксированных системой интегрального мониторинга в ИС, – один из наглядных показателей эффективности функционирования СУИБ. Внедрение процесса управления инцидентам ИБ позволяет количественно оценить эту эффективность.

Для внедрения процедуры управления инцидентами ИБ необходимо провести следующие организационно-технические мероприятия.

1. *Утвердить процедуры разработки управления инцидентами ИБ* (как и всех процедур в организации) по инициативе ее руководства. Как правило, процедура управления инцидентами разрабатывается в рамках внедрения СУИБ, поэтому важна позиция руководства по вопросу ее создания и функционирования. На данном этапе важно, чтобы все сотрудники организации понимали, что обеспечение информационной безопасности в целом и управление инцидентами ИБ в частности являются основными бизнес–целями организации.

2. *Разработать необходимыенормативные документы по управлению инцидентами*. Такие документы должны описывать:

– определение инцидента ИБ, перечень событий, являющихся инцидентами ИБ (что в организации является инцидентом);

– порядок оповещения ответственных лиц о возникновении инцидента ИБ (необходимо определить формат отчета, а также отразить

контактную информацию лиц, которых следует оповещать об инциденте);

– порядок устранения последствий и причин инцидента ИБ;

– порядок расследования инцидента ИБ (определение причин инцидента ИБ, виновных в возникновении инцидента ИБ, порядок сбора и сохранения улик);

– внесение дисциплинарных взысканий;

реализация необходимых корректирующих и превентивных мер.

3. О*пределить понятие инцидента ИБ, так как в* организации отсутствует методика определения инцидентов ИБ, а сотрудники не знают, какие события являются инцидентами ИБ. Следует понимать, что все события, которые не войдут в указанный перечень, будут рассматриваться как штатные (даже если они несут угрозу информационной безопасности). В частности, инцидентами ИБ могут быть:

– отказ в обслуживании сервисов, средств обработки информации, оборудования;

– нарушение конфиденциальности и целостности ценной информации;

– несоблюдение требований к ИБ, принятых в организации (например, нарушение правил обработки информации);

– несанкционированный мониторинг ИС;

– вредоносные программы;

– компрометация ключевой системы (например, разглашение пароля пользователя).

Поскольку инцидентом ИБ является неразрешенное событие, оно должно быть запрещено, следовательно, необходимо разработать документ, в котором четко классифицированы инциденты ИБ, описаны все действия, которые можно выполнять в ИС пользователю и которые выполнять запрещено. Важно, чтобы были налажены такие процедуры, как интегральный мониторинг событий безопасности, своевременное удаление неиспользуемых учетных записей, контроль действий легальных пользователей в ИС, в том числе привилегированных, и пр.

4. *Разработать процедуру* о*повещения о возникновении инцидента ИБ.* Сотрудники организации зачастую не осведомлены о том, кого и в какой форме следует ставить в известность при возникновении инцидента, — например, не определены ни формы отчетов, ни перечень лиц, которым необходимо отправлять отчеты об инцидентах. Даже если сотрудник заметит, что его коллега уносит для работы домой конфиденциальные документы организации, он не всегда знает, какие действия следует предпринимать в данной ситуации.

5. Разработать методику *регистрации инцидента ИБ.*Ответственным лицам (даже если таковые назначены) часто не предоставляется методика регистрации инцидентов — не существует специальных журналов их регистрации, а также правил и сроков заполнения.

Требуется разработать инструкцию для специалиста, в обязанности которого входит регистрация инцидента. Сотрудник, обнаруживший инцидент, связывается с сотрудником, ответственным за регистрацию инцидента и выполнение дальнейших действий. В небольших организациях сотрудники обращаются напрямую к специалисту, который может устранить последствия и причины инцидента (например, к системному администратору или администратору безопасности). В достаточно крупных организациях, как правило, выделяют сотрудника, который регистрирует инцидент и передает информацию об инциденте соответствующим специалистам. Такая инструкция может содержать, например, правила и срок регистрации инцидента, перечень необходимых первоначальных инструкций для сотрудника, обнаружившего инцидент, кроме того, описание порядка передачи информации об инциденте соответствующему специалисту, порядок контроля за устранением последствий и причин инцидента.

6. Разработать процедуру у*странения последствий и причин инцидента ИБ*. В организациях, как правило, отсутствует документально зафиксированная процедура, описывающая действия, которые необходимо выполнить с целью устранения последствий и причин инцидента. В первую очередь такая процедура должна предусматривать, чтобы мероприятия по устранению последствий и причин инцидента не нарушали процедуры их расследования: устранение последствий инцидента не должно «заметать следы», чтобы невозможно было установить виновных в инциденте.

Инструкция по устранению причин и последствий инцидента включает описание общих действий, которые необходимо предпринять (конкретные действия для каждого вида инцидента определять трудоемко и не всегда целесообразно), а также сроки, в течение которых следует устранить последствия и причины инцидента. Сроки устранения последствий и причин инцидента зависят от уровня инцидента. Следует разработать классификацию инцидентов – определить количество уровней критичности инцидентов, описать инциденты каждого уровня и сроки их устранения. Документ, определяющий, какие события в организации следует считать инцидентом, также может описывать и уровни инцидентов.

Таким образом, инструкция по устранению последствий и причин инцидента может включать: описание действий, предпринимаемых для устранения последствий и причин инцидента, сроки устранения и указание на ответственность за несоблюдение инструкции.

7. Разработать Инструкцию по *расследованию инцидента ИБ*. На этапе расследования инцидентов основную роль играют: ведение журналов регистрации событий, четкое разделение полномочий пользователей, ответственность за выполненные действия – важны доказательства того, кто участвовал в инциденте и какие действия он выполнял.

Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий. В крупных организациях, как

правило, выделяют комиссию по расследованию инцидентов информационной безопасности (в состав которой может входить сотрудник, регистрирующий инциденты). Инструкция по расследованию инцидентов должна описывать: действия по расследованию инцидента (в том числе определение виновных в его возникновении), правила сбора и хранения улик (особенно в случае, если может потребоваться использование улик в судебных органах) и правила внесения дисциплинарных взысканий.

Как правило, если организации был нанесен какой–либо ущерб, то к виновным в возникновении инцидента (которые определены без необходимых в таких случаях процедур) все же применяются различные взыскания, однако внесение дисциплинарных взысканий не всегда подчиняется утвержденным процедурам и другие действия по предотвращению повторения инцидента выполняются тоже не всегда.

После устранения последствий инцидента и восстановления нормального функционирования бизнес–процессов организации, возможно, потребуется выполнить действия по предотвращению повторного возникновения инцидента. Для определения необходимости реализации таких действий следует провести анализ рисков, в рамках которого определяется целесообразность корректирующих и превентивных действий.

Через определенное время (как правило, через полгода или год) необходимо заново пересмотреть перечень событий, называемых инцидентами, форму отчета и пр., внедрить обновленную процедуру в информационную систему, проверить ее функционирование и эффективности и реализовать превентивные действия. Таким образом, цикл модели PDCA будет непрерывно повторяться и гарантировать четкое функционирование процедуры управления инцидентами и, главное, ее постоянное улучшение.

Во многих крупных организациях внедряется служба поддержки Service Desk, в обязанности которой входит управление инцидентами в области информационных технологий. Процедура управления ИТ–инцидентами регулируется стандартом ISO/IEC 20000:2005, пришедшим на смену BS 15000:2002, который, в свою очередь, взял за основу библиотеку ITIL. Сама процедура управления инцидентами ИТ очень близка к процедуре управления инцидентами ИБ с той лишь разницей, что в последнем случае больший упор делается на его расследование, сбор улик, наказание виновных (вплоть до обращения в суд).

Управление инцидентами ИБ, как правило, возлагается на службу поддержки, обрабатывающую инциденты ИТ (в том случае, если такая служба существует в организации). Это еще раз доказывает то, что целесообразно разработать одну систему управления всеми процессами в организации, так как управление схожими процессами в разных областях ее деятельности часто выполняется по одной схеме

Важно, чтобы ни один инцидент ИБ не остался незамеченным, было проведено расследование, выявлены виновные, и, самое главное, выполнены

корректирующие и превентивные действия. Главной особенностью инцидентов ИБ является то, что они не всегда заметны (не всегда мешают в работе пользователей), однако возможный ущерб от таких инцидентов сложно недооценить. Следовательно, необходима четкая процедура регистрации и расследования инцидентов безопасности, а также информирование пользователей о правилах определения инцидентов ИБ.

Необходимо понимать, что управление инцидентами ИБ не предупреждает нанесение ущерба организации (как правило, организация уже понесла ущерб, связанный с инцидентом), однако расследование инцидента ИБ и своевременное внедрение превентивных и корректирующих мер снижает вероятность его повторения (и, следовательно, вероятность повторения нанесения ущерба). Отметим также, что статистика инцидентов ИБ представляет особую ценность для организации как показатель эффективности функционирования СУИБ. Статистику инцидентов ИБ следует также регулярно анализировать в рамках аудита системы управления информационной безопасностью.

5.3.3. Внедрение системы интегрального мониторинга ИБ

После проведения анализа рисков, выбора и внедрения контрмер, необходимо оценить их эффективность. Как правило, эффективность внедренных средств защиты определяется с помощью повторного анализа рисков. Необходимо понять, насколько действительно снизился риск. *Внедрение системы интегрального мониторинга ИБ направлено на решение задачи обеспечения постоянного контроля эффективности контрмер* (контроля рисков) для периодической переоценки рисков. Таким образом, суть контроля эффективности контрмер состоит в том, чтобы убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Критерием эффективности внедренных контрмер может служить, например, количество и частота зафиксированных инцидентов ИБ за определенный временной период. При реализации *системы интегрального мониторинга ИБ* рекомендуется использовать ГОСТ Р ИСО/МЭК ТО 18044.

На этапе «ПЛАНИРОВАНИЕ» было определено, что система интегрального мониторинга информационной безопасности (ЕСМИБ) должна обеспечить

– полноту и непрерывность сбора первичных событий ИБ от объектов области действия СОИБ с целью идентификации инцидентов ИБ;

– процедуру формирования оценки ИБ и ведения базы данных коррелированных событий ИБ;

– выработку рекомендаций по оперативному блокированию инцидентов ИБ;

– проведения отложенного анализа интегральных событий ИБ.

Приведем краткий обзор рынка систем интегрального мониторинга ИБ зарубежного и отечественного производства

5.3.3.1. Система сбора, анализа и корреляции информации netForensics

Система netForensics производства организации netForensics [56] предназначена для сбора, анализа и корреляции информации, поступающей от средств обнаружения попыток НСД, маршрутизаторов, МЭ, ОС, VPN и WEB- серверов. Устройства, которые не поддерживаются системой, могут быть легко интегрированы при помощи универсальных агентов. Информация, поступающая от устройств, подвергается четырём стадиям обработки: нормализация, агрегация, корреляция и визуализация.

На этапе нормализации каждое сообщение преобразуется в одно из ста внутренних сообщений системы.

На этапе агрегации, последовательности событий группируются на основе одного или нескольких критериев. В качестве критериев могут выступать: адрес источника, порт источника, адрес получателя, порт получателя, тип события, тип источника, протокол передачи, процесс, текст сообщения.

Далее, данные подвергаются корреляции. В системе реализовано два механизма корреляции – статистическая и корреляция, основанная на правилах. Статистическая корреляция позволяет проводить оценку рисков. Корреляция, основанная на правилах, позволяет создавать событие, соответствующее реализации определённого сценария атаки, определяемого как последовательность событий, сгруппированных по определённым признакам с помощью логических операций.

После процессов нормализации, агрегации и корреляции, консолидированные данные отображаются в реальном времени на консоли.

Система реализована в трёхзвенной архитектуре, что даёт большие возможности масштабируемости, распределения компонентов и повышения надёжности. Основные компоненты системы – агенты, engines, master engine, консоль, база данных.

Функции агентов – приём данных, нормализация, преобразование в формат XML и передача по защищённому соединению engine. Engine агрегирует и коррелирует полученные от агентов данные. Master engine агрегирует и коррелирует данные полученные от engine (возможна конфигурация с несколькими engine). Консоль отвечает за отображение данных.

Все соединения между компонентами системы защищены. netForensics имеет гибкую систему генерации отчётов. Возможно создание пользовательских отчётов, и имеется большое количество предопределённых. Формат отчётов – HTML, CVS, PDF. Имеется возможность ролевого управления.

В качестве СУБД используется промышленная СУБД Oracle9i. Поддерживаемые ОС – Windows, Solaris, Linux.

5.3.3.2. Система сбора, анализа и корреляции информации EnVision

Система EnVision производства организации Network-Intelligence [57] предназначена для сбора, анализа и корреляции информации, поступающей

от средств обнаружения попыток НСД, маршрутизаторов, МЭ, ОС, VPN. В отличие от netForensics, в enVision реализован единственный механизм корреляции – корреляции, основанной на правилах.

Система принимает все сообщения на порт №514 (нет возможности изменения без обращения в службу поддержки) по протоколу UDP. Далее сообщения записываются в файл, и, через настраиваемый интервал времени, записываются в базу данных.

EnVision имеет двухзвенную архитектуру и нет возможности распределения компонентов. Система генерации отчётов позволяет создавать пользовательские отчёты и имеет около 350 предопределённых. Формат отчётов – HTML.

Основные компоненты системы: DashBoard, Event Viewer, Alert Monitor, Alert Browser, Report VU. DashBoard позволяет контролировать состояние компонентов системы. Event Viewer – консоль, позволяющая просматривать сообщения в реальном масштабе времени. Alert Monitor предназначен для просмотра коррелированных событий и событий, определённых в представлениях (views). Alert Browser позволяет просматривать сообщения, которые были сохранены в базе данных. Report VU – система генерации отчётов. Система имеет WEB интерфейс.

В системе реализован один вид корреляции – корреляция, основанная на правилах. Система не производит нормализацию сообщений, как система netForensics, и поэтому правила определяются для конкретных сообщений устройств. Каждое правило имеет следующие общие параметры:

– Message ID – идентификатор сообщения;

– Message text – текст сообщения;

– Class – класс корреляционного правила;

– Category – категория, соответствующая классу правила;

– Decay time – время, в течении которого должны произойти все события;

– Level – значимость сообщения (от 0 до 7);

– IP address matching – условие на IP адреса, обнаруженные в сообщениях;

Description – описание правила;

– Action – действие при соответствии полученной информации корреляционному правилу;

Последовательность сообщений, образующих правило – одно или несколько Circuit (совокупность операций), связанных одним из операторов:

– Or (или);

– And (и);

– And not (и не);

– Or not (или не);

– Followed by (следует за).

Временное действие каждого оператора можно ограничить (по умолчанию – бесконечность), после окончания заданного интервала

состояние правила сбрасывается в начальное.

В системе имеется около 350 предопределённых отчётов. Все отчёты распределены по группам. Процесс создание пользовательских отчётов – пошаговое создание SQL запроса к базе данных с помощью графического интерфейса. Возможна генерация отчётов по расписанию.

5.3.3.3. Система управления средствами защиты, анализа и корреляции ISS RealSecure SiteProtector

ISSRealSecureSiteProtector производства организации ISS [58] предназначена для управления средствами защиты, производимыми организацией ISS, анализа и корреляции поступающих данных. С помощью Third Party Module возможно получение информации от МЭ Cisco PIX и CheckPoint FW. При использовании Fusion Module возможно осуществление корреляции данных, поступающих от ПО Network Sensor, Server Sensor и Internet Scanner.

Отличительная особенность системы – возможность корреляции данных об атаках с информацией о реальных уязвимостях, полученной после сканирования с помощью ISS Internet Scanner.

Система имеет распределённую архитектуру, что даёт большие возможности для распределения компонентов, масштабируемости и повышения надёжности. Основныекомпонентысистемы: DataBase, Application Server, Sensor Controller, Event Collector, Console, Fussion Module, Third Party Module исенсоры (Network Sensor, Server Sensor ит.д.) DataBase – база данных, которая отвечает за хранение всех данных, циркулирующих в системе. Application Server – сервер приложений, отвечающий взаимодействие компонентов. Event Collector отвечает за приём информации от сенсоров и передачу в СУБД. Console – приложение, которое позволяет управлять, конфигурировать и просматривать информацию о состоянии компонентов системы и отображать информацию о событиях, зарегистрированных сенсорами. Fussion Module отвечает за корреляцию данных, поступающих от сенсоров. Third Party Module предназначен для получения сообщений от МЭ Cisco PIX и CheckPoint FW.

Все соединения между компонентами системы защищены.

В качестве СУБД используется MS SQL Server 2000 или MSDE.

Система обрабатывает события, поступающие от ПО ISS Network Sensor, Server Sensor, Desktop Protector, System Scanner, Internet Scanner, а также ПО МЭ Cisco PIX и CheckPoint FW.

Механизмы корреляции реализуется модулем Security Fusion Module. В системе реализовано два механизма корреляции:

– Event Correlation – корреляция информации об атаках и реально существующих уязвимостях;

– Attack Correlation – корреляция, основанная на правилах.

Отличительной особенностью системы является наличие механизма Event Correlation. Механизм Event Correlation реализуетсякомпонентом

Impact Analysis Component модуля Security Fusion Module. Работа этого механизма позволяет уменьшить количество бесполезной информации на консоли системы. Это достигается путём изменения приоритета события от значения, заданного в политиках сенсора. Основываясь на результатах сканирования с помощью Internet Scanner, подключенного к системе ISS SiteProtector, и информации, поступающей от сенсоров, IAC может оценить возможность реализации атаки, и затем выполнить одно или несколько действий из следующего списка:

– изменить приоритет события;

– записать событие в базу данных;

– отобразить информацию о событии на консоли;

– послать электронное письмо;

– послать SNMP;

– реакция, определённая пользователем.

Механизм AttackCorrelationреализуется компонентом AttackPatternComponentмодуля SecurityFusionModule. Данная корреляция – корреляция, основанная на правилах. Работа этого механизма позволяет сопоставить информацию от многих сенсоров предопределённых шаблонам атак и определить наличие таких событий, как попытки вторжения (в том числе и происходящие в «несколько шагов»), несанкционированное сканирование и прочие. Также модуль позволяет уменьшить количество информации на консоли путём комбинирования данных, полученных от многих сенсоров, которые соответствуют одному и тому же событию.

При минимальном соответствии полученных данных одному из шаблонов, модуль создаёт инцидент. Если при дальнейшем анализе будут получены данные, связанные с уже обнаруженным инцидентом, они будут добавлены к существующему.

Возможно создание исключений (Exception) из определённых событий или инцидентов. Событие или инцидент, добавленные в исключение, убираются из дальнейшего рассмотрения системой.

В системе реализовано 20 шаблонов атак. Возможности создания собственных шаблонов нет.

Система генерации отчётов позволяет создавать отчёты, соответствующие текущему представлению данных на консоли. Формат отчётов – HTML, CVS, PDF.

5.3.3.4. Система визуального анализа данных VisualLinks

Организация VisualAnalyticsInc. [59] является лидером в области разработки программных продуктов визуального анализа данных и извлечения знаний (Visual Data Mining), организации информационного взаимодействия и коллективной работы аналитиков. Решения организации Visual Analytics Inc.

VisuaLinks – платформенно-независимый инструмент визуального анализа данных, используемый для выявления шаблонов, тенденций,

взаимосвязей и скрытых закономерностей в любых по типам и объемам источниках данных. VisuaLinks поддерживает полный цикл анализа информации – от обеспечения доступа к информационным источникам и их интеграции до создания отчетных документов, и представления результатов анализа. VisuaLinks предлагает единое и полное решение для широкого класса аналитических задач. VisuaLinks включает широкий набор инструментов и позволяет:

– объединять множество баз данных, имеющих различный формат и территориальное расположение;

– отображать неограниченные объемы данных;

– выявлять прямые и косвенные связи между объектами;

– обеспечить прямой доступ к любым базам данных без перезагрузки информации;

– раскрывать пересечения и взаимосвязи между различными типами данных;

– графически представлять результаты анализа в виде схем и диаграмм;

– использовать мощные аналитические функции для выявления шаблонов и тенденций;

– проводить расследование в упреждающем режиме;

– поддерживать работу аналитических групп в режиме on-line;

– сохранять данные в различных форматах, включая базы данных, HTML, XML, изображения и текстовые файлы.

VisuaLinks поддерживает архитектуру клиент-сервер, что позволяет пользователям проводить анализ и обмениваться различными типами информации в ходе выполнения широкого круга задач. Объектами для данной системы может служить любая предметная область. Для обеспечения эффективного формирования наблюдаемых объектов VisualLinks предоставляет средства, позволяющие провести:

– разработку унифицированных подходов к формированию описания предметной области;

– формирование требуемого набора объектов и связей, адекватно описывающих предметную область;

– разработку правил идентификации поступающей информации по объектам учета и ее сопоставления с хранящимися в системе данными.

Решение первых двух задач позволяет при работе с системой оперировать понятиями предметной области. В качестве элементов предметной области могут выступать типы объектов и связей. В качестве источников информации могут выступать информационные ресурсы, такие как:

– «витрины» (представления) данных из любых типов хранилища данных;

– БД, содержащие информацию службы электронного почтового обмена, а также сведения о компьютерных вирусах, нарушителях, отпусках сотрудников;

– при необходимости, дополнительные БД любых форматов, поддерживающих JDBC или ODBC интерфейс (Oracle, MS SQL Server, MS Access, DB2, MySQL и т.п.).

Система VisualLinks при функционировании обеспечивает поддержку следующих основных этапов выявления нарушений:

– формирование информационных массивов для целей анализа;

– оперативная обработка и анализ информации;

– представление результатов расследования.

Формирование информационных массивов для целей анализа – это этап сбора информации, достижение ее понимания и определение релевантности связей каждого элемента со всеми остальными. На данном этапе ведется целенаправленный сбор информации при помощи различных средств из всех доступных источников. Использование современных технологий позволит концентрировать усилия на сборе конкретной информации, относящейся к текущей деятельности. Данный элемент процесса расследования имеет важнейшее значение для работы всей системы, поскольку он позволяет минимизировать непроизводительные затраты времени и ресурсов. В рамках формирования информационных массивов для целей комплексного анализа обеспечивается информационно-аналитическая поддержка следующих процессов:

– извлечение, преобразование и загрузка данных;

– хранение данных.

Оперативная обработка и анализ информации – это объективный анализ результатов этапа формирования информационных массивов для достижения понимания целого. Данный этап является ключевым и включает:

– поиск значимых информационных объектов и связей;

– выявление признаков нарушений;

– проведение интерактивного детального анализа данных;

– выявление скрытых связей и закономерностей;

– проверка версий, выдвинутых в процессе выявления, раскрытия и расследования инцидентов, формирование направлений дальнейших действий.

Представление результатов расследования, формально, - это передача достигнутого понимания пользователям с целью практического использования полученных сведений. Система комплексного анализа обеспечивает представление результатов расследования (в том числе визуальное) в виде отчетов, схем, таблиц, графиков и диаграмм.

Подход к интегральному анализу данных системы VisualLinks включает (рис.5.2):

– Методы и инструменты выявления закономерностей (Data Mining) предназначены для автоматизированного первичного отбора информации, содержащей признаки нарушений при использовании критических ресурсов.

– Инструменты многомерного анализа статистических данных (OLAP) позволяют получать регламентированные отчеты, строить

нерегламентированные запросы и отчеты, извлекать и представлять аналитическую информацию в нужных разрезах и форматах, осуществлять переходы от агрегированных данных к детальным.

– Визуальный анализ предназначен для проведения интерактивного детального анализа всей совокупности информации, относящейся к расследуемым инцидентам.

Технологии анализа неструктурированной информации позволяют визуализировать информацию в документе, представляя ее в легком для понимания виде. Для этого сотрудник выделяет значимые части текста в документе и на основе их создает объекты и связи на схеме. Созданные таким образом сущности могут быть сохранены в базе данных и использоваться для дальнейшего анализа.

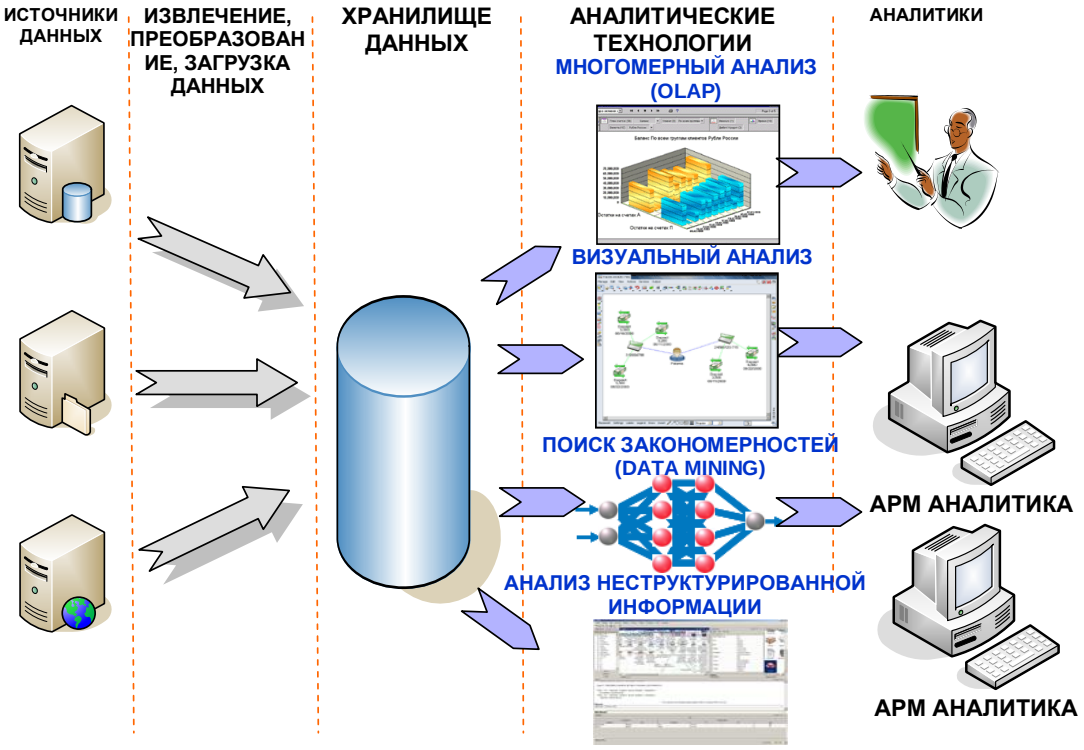

Рис.5.2. Подход к интегральному анализу данных системы VisualLinks

По мнению организации, традиционные методы Data Mining эффективно работают на этапе первичного отбора информации, содержащей признаки правонарушений (преступлений и административных правонарушений). Технологии OLAP обеспечивают аналитикам возможность исследовать большие объемы взаимосвязанных данных при помощи быстрого интерактивного их отображения на разных уровнях детализации с различных точек зрения в соответствии с представлениями конечного пользователя. Наряду с Data Mining, технологии OLAP позволяют определить направление детального исследования информации с помощью инструментов визуального анализа данных.

VisualLinks предоставляет пользователям развитый инструментарий, с

помощью которого они могут самостоятельно, не прибегая к услугам программистов, формировать нужные отчетные документы и аналитические материалы. Основной формой отчета является схема взаимосвязанных объектов. Схемы могут быть различных видов:

– схемы ролевых связей – событие (факт) представляется в виде объекта, с которым на различных ролях связаны другие объекты. Данный способ используется для распознавания следующих схем: точки пересечения, локальные объекты, изолированные кластеры, сильно/слабосвязанные группы, цепочки, общности;

– схемы потоков (почтовых сообщений, финансовых, телефонных звонков и т.п.) - событие (факт) представляется в виде связи, соединяющей два объекта (например, отправителя и получателя, или счета кредита и дебета, или плательщика и получателя). Данный способ используется для распознавания следующих схем: изолированные кластеры, сильно/слабосвязанные группы, цепочки, потоки;

– комплексные схемы – объединяет на одной схеме различные виды представления событий (фактов). Данный способ позволяет избежать «лавинообразное» увеличение количества объектов на схеме (характерное для представления в виде схем ролевых связей) и получить исчерпывающую картину (что не всегда возможно для представления в виде потоков связей).

5.3.3.5. Сравнительный анализ подходов к интегральному анализу данных мониторинга ИБ зарубежных систем

Сравнительный анализ подходов к интегральному анализу данных мониторинга ИБ зарубежных систем показывает, что:

– рассмотренные системы, реализующие подходы к интегральному анализу данных мониторинга, имеют либо распределенную, либо клиент-серверную архитектуру. Вид архитектуры зависит от источников данных мониторинга: если источниками данных мониторинга являются уже сформированные базы данных, файлы и т. д. (нет необходимости в сборе данных мониторинга), то подход к интегральному анализу реализуется на основе клиент-серверной архитектуры;

– наблюдаемыми объектами для интегрально анализа данных мониторинга, как правило, являются пользователи и элементы наблюдаемых автоматизированных систем. Исключение составляет система VisualLinks, в которой имеется возможность задания типов наблюдаемых объектов в зависимости от области применения данного средства;

– интегральный анализ данных мониторинга выполняется в три этапа: сбор данных мониторинга (включает в себя непосредственный съем информации, ее консолидацию и агрегацию), анализ (сигнатурный и статистический) и формирование отчета;

– методы, используемые при интегральном анализе данных мониторинга, как правило, ориентированы на выявление корреляции, основанной на правилах (сигнатурный анализ). Исключение составляют

системы netForensics и VisualLinks, позволяющие использовать для анализа статистический аппарат и развитую систему визуализации (только VisualLinks);

– рассмотренные системы, реализующие подходы к интегральному анализу данных мониторинга, имеют развитые подсистемы генерации отчетов, предлагающие до несколько сотен видов отчетов (netForensics и EnVision). Подсистемы генерации отчетов предлагают также развитый сервис визуализации (только VisualLinks).

Следует учитывать, что характерными недостатками систем являются: отсутствие локализации, отсутствие эксплуатационной документации на русском языке, высокая стоимость и сложность настройки и технической поддержки.

5.3.3.6. Обоснования выбора систем мониторинга отечественного производства [21]

Системы мониторинга ИБ являются одним из компонентов систем контроля защищенности информационных инфраструктур РФ.

Под стандартными продуктами понимается покупное ПО в основном западных фирм-производителей, сравнительно широко растиражированное за рубежом и получившее определенное признание в России. Некоторые из таких продуктов достаточно давно применяются и в России, например, HP Open View. Универсальный характер ряда стандартных продуктов, в принципе, позволяет использовать их не только по прямому назначению – для целей оптимизации ИТ инфраструктуры, сетей, учета конфигураций, контроля работы сервисов и технологий, и т. п. Из-за наличия ряда хорошо отработанных решений на базе стандартных продуктов для ИТ-инфраструктур идея создать и внедрить аналогичные решения для ИБ порой кажется весьма привлекательной и даже соблазнительной. При этом по умолчанию ошибочно предполагается, что задачи в области ИБ аналогичны таким задачам, как контроль сервисов и технологий в области ИТ–инфраструктур.

Например, при анализе одного и того же инцидента ИТ-подразделение интересуют условия его возникновения, оценка потребленного ресурса (информационные потоки на входе и выходе, нагрузка на систему) и соотношение с имеющимися ресурсными возможностями (такими как пропускная способность каналов, производительность системы и другими), а также другие количественные оценки, позволяющие разобраться в возникшей ситуации и устранить последствия. При этом предполагается, что причина инцидента техническая или организационная, во всяком случае, злоумышленная активность не рассматривается или рассматривается в последнюю очередь.

Службу ИБ интересуют ответы хотя бы на три вопроса, связанные с этим же инцидентом:

– Какие свойства безопасности информационных активов были

нарушены?

– Какой ущерб нанесен и его величина.

– Не является ли произошедший инцидент следствием злоумышленной активности?

Для ответа на эти вопросы требуется углубленный анализ предшествующих и последующих событий с целью поиска причинно-следственных связей между ними. Обеспечение информационной безопасности на основе методологического базиса агентных технологий рассмотрен, например, в [60-62]. Также необходимы подробные сведения о затронутых активах и операциях с ними, причастном персонале и т. п., т. е. обо всем, что образует контекст события-инцидента.

Ниже рассматриваются причины, препятствующие созданию решений в области ИБ на основе стандартных продуктов, в частности, причины выбора для целей контроля действий администраторов и пользователей решений, на основе разрабатываемых российских специализированных систем в противовес решениям на базе стандартных продуктов ведущих иностранных производителей [РИ]. При этом рассматривается только техническая сторона вопроса, хотя можно предположить, что экономическая сторона вопроса, при попытке решить проблему доработки стандартного импортного продукта, также окажется существенным фактором.

1. Необходимость получения событий мониторинга ИБ от новых источников или применения новых способов сбора (доставки) информации о событиях (специализированных интерфейсов, нетиповых протоколов).

В разрабатываемых российских системах мониторинга ИБ возможность подключения новых источников данных решается в рамках функционального развития этих систем после согласования Заказчиком предлагаемых решений.

Реализовать подобные решения в стандартных импортных продуктах можно силами подрядных организаций за счет создания ПО так называемых «адаптеров», выполняющих функции конвертирования событий мониторинга ИБ из журналов ИС (т.е. новых источников) во внутренний формат продукта. Как правило, стандартные импортные продукты предоставляют возможности написания адаптеров, публикуя для этого API, однако, при создании адаптера для журналов конкретной системы предоставленных возможностей может оказаться недостаточно и возникнет необходимость привлечения производителя продукта. Однако в силу разных причин создать новые адаптеры невозможно.

Проблема получения информации от новых источников в условиях России, когда используется покупное ПО, разработанное с учетом западных стандартов, весьма актуальна. И особенно это актуально для продуктов, применяемых в области ИБ, поскольку по Российскому законодательству в некоторых областях, например, связанных с криптографией, использовать зарубежные аппаратные средства и ПО просто нельзя. В стандартных

продуктах не предусмотрена возможность импорта и анализа регистрационных журналов от российских средств ИБ.

2. Необходимость получения дополнительной информации об условиях и ситуации, связанной с возникновением событий (установления контекста событий), вызванная спецификой анализа и оценки событий ИБ, а также адекватной их интерпретацией.

Для установления контекста событий ИБ чаще всего требуется сбор дополнительных событий мониторинга, связанных с этим контекстом. Возможности сбора дополнительных событий мониторинга ИБ, как правило, в принципе не могут быть решены для стандартных импортных продуктов написанием адаптеров, поскольку требуют специальных возможностей, например, перехвата системных вызовов в ОС.

Адаптеры стандартных продуктов предназначены только для изменения формата представления события мониторинга ИБ из штатных журналов приложений ИС, но никак не могут заменить формирование новых событий и при необходимости взять дополнительную информацию, необходимую для контроля и анализа, путем перехвата системных вызовов.

Проблема установления контекста возникает из-за неопределенностей и неоднозначности информации, связанной с событиями, регистрируемыми в штатных журналах регистрации платформ и приложений. А именно, события с одним и тем же кодом генерируются по разным ситуациям, возникшим в системе, программе, приложении. При этом предполагается, что этой информации достаточно, поскольку основным назначением такой записи в журнале регистрации является просто сигнал о нештатной (или штатной) ситуации. Если необходимо в этой ситуации разобраться подробнее, например, найти ошибку или другую причину ее возникновения, то ситуация должна быть повторена, а программное обеспечение при этом должно быть переведено в специальный отладочный режим с подробным протоколированием промежуточных данных, трассировкой исполнения программы или системных вызовов и т. п. Затем отладочная информация (фактически контекст события) анализируется специалистами разработчика ПО на стендах. Таким образом, контекст события при необходимости формируется и анализируется в «лабораторных» условиях.

Но эта схема не подходит для целей безопасности потому, например, что ситуацию, специально созданную злоумышленником, можно, с применением какого-то уникального инструментария, повторить невозможно. Она возникает один раз во время проведения атаки. Весьма примечательно, что цели безопасности не учитываются разработчиками ПО даже в тех случаях, когда дополнительная информация о событии могла бы быть включена без особых затрат.

3. Необходимость контроля работы приложений, не формирующих собственный журнал регистрации событий.

Если по условиям вновь утвержденной или введенной в действие политики ИБ возникает потребность контроля приложений ИС, не

формирующих собственного журнала регистрации событий, то такая ситуация принципиально неразрешима с использованием стандартных импортных продуктов, поскольку приводит к необходимости формирования нужных для контроля событий средствами этого продукта. Здесь единственной возможностью для получения событий мониторинга ИБ является перехват системных вызовов.

Возможность доработки стандартных импортных продуктов в части формирования новых событий, не генерируемых штатными средствами регистрации ОС и приложений, ограничена. Кроме того, в подавляющем большинстве случаев, при необходимости контроля приложений ИС, не формирующих собственных регистрационных журналов, требуется участие разработчиков стандартного продукта.

4. Необходимость в специализированных средствах анализа и генерации отчетов, потребности их доработки, переработке и оптимизации.

При использовании специализированных средств разрабатываемых российских систем мониторинга ИБ такая оптимизация или доработки предусматриваются в рамках сопровождения или функционального развития.

Возможности анализа и отчетности в стандартных продуктах также ограничены. Доработка или адаптация видов отчетности по пожеланиям Заказчика требуют участия разработчиков и вряд ли возможны.

5. Необходимость защиты данных мониторинга от таких угроз как:

– действия администраторов по отключению процессов, осуществляющих сбор данных о событиях мониторинга ИБ;

– модификация, уничтожение данных о событиях мониторинга ИБ;

– подмена актуальных данных данными, сформированными ранее.

В системах контроля действий администраторов и пользователей отечественной разработки возможна реализация комплекса мер противодействия данным угрозам.

Кроме того, в отечественных разработках систем указанного класса (например, ПАО «Информзащита» – г. Москва, НПФ «Кристалл» – г. Пенза) проектные решения предусматривают децентрализованный сбор данных мониторинга ИБ, т. е. имеется возможность за счет автономной работы средств сбора осуществлять контроль действий пользователей выделенных объектов или их групп.

5.3.3.7. Единая система мониторинга информационной безопасности НПФ «Кристалл» (г. Пенза)

Среди российских кампаний, ведущих разработки в данном направлении можно выделить НИЦ «Информзащита» (г. Москва) и НПФ «Кристалл» (г. Пенза). Рассмотрим подходы к реализации интегрального мониторинга ИБ на примере единой системы мониторинга информационной безопасности для территориальных отделений Банка России (ЕСМИБ ТУ) НПФ «Кристалл»

[44].

ЕСМИБ ТУ предназначена для автоматизации контроля выполнения требований нормативных и иных документов Банка России по информационной безопасности (ИБ) на объекте автоматизации пользователями автоматизированных систем (АС), в том числе в рамках проведения процедур внутреннего контроля уровня территориального учреждения Банка России (ТУ Банка России).

ЕСМИБ ТУ является трех уровневой системой и состоит из следующих подсистем (рис.5.3.):

а) *Первый уровень мониторинга ИБ* – уровень сбора первичных событий мониторинга и контроля отчуждения информации:

– подсистема сбора первичных событий мониторинга (далее по тексту – подсистема сбора данных);

– подсистема контроля отчуждения информации (далее по тексту – подсистема контроля отчуждения);

б) *Второй уровень мониторинга ИБ* – уровень формирования сообщений о событиях ИБ:

– подсистема анализа и формирования сообщений о событиях ИБ (далее по тексту – подсистема анализа);

– подсистема хранения событий ИБ;

– подсистема информирования о событиях ИБ (далее по тексту – подсистема информирования);

– подсистема расследования событий ИБ (далее по тексту – подсистема расследования);

в) *Третий уровень мониторинга ИБ* – уровень формирования и обработки КСИБ:

– подсистема идентификации КСИБ;

– подсистема импорта исходных данных;

– подсистема обработки КСИБ;

– подсистема хранения и резервирования КСИБ;

– подсистема подготовки отчетов по КСИБ;

– подсистема централизованного обновления базы требований документов Банка России по ИБ.

Подсистема сбора данных предназначена для автоматизированного сбора первичных событий мониторинга из журналов ШПРС подконтрольных объектов, а также их регистрации.

Подсистема анализа предназначена для автоматизированного анализа первичных событий мониторинга (входных данных) из журналов ШПРС подконтрольных объектов и формирования сообщений о событиях ИБ по заданным правилам с целью оценки степени их влияния на ИБ объекта автоматизации.

Подсистема контроля отчуждения предназначена для фиксации первичных событий мониторинга о работе персонала объекта автоматизации

со съемными периферийными устройствами на подконтрольных объектах, работающих под управлением ОС Microsoft Windows.

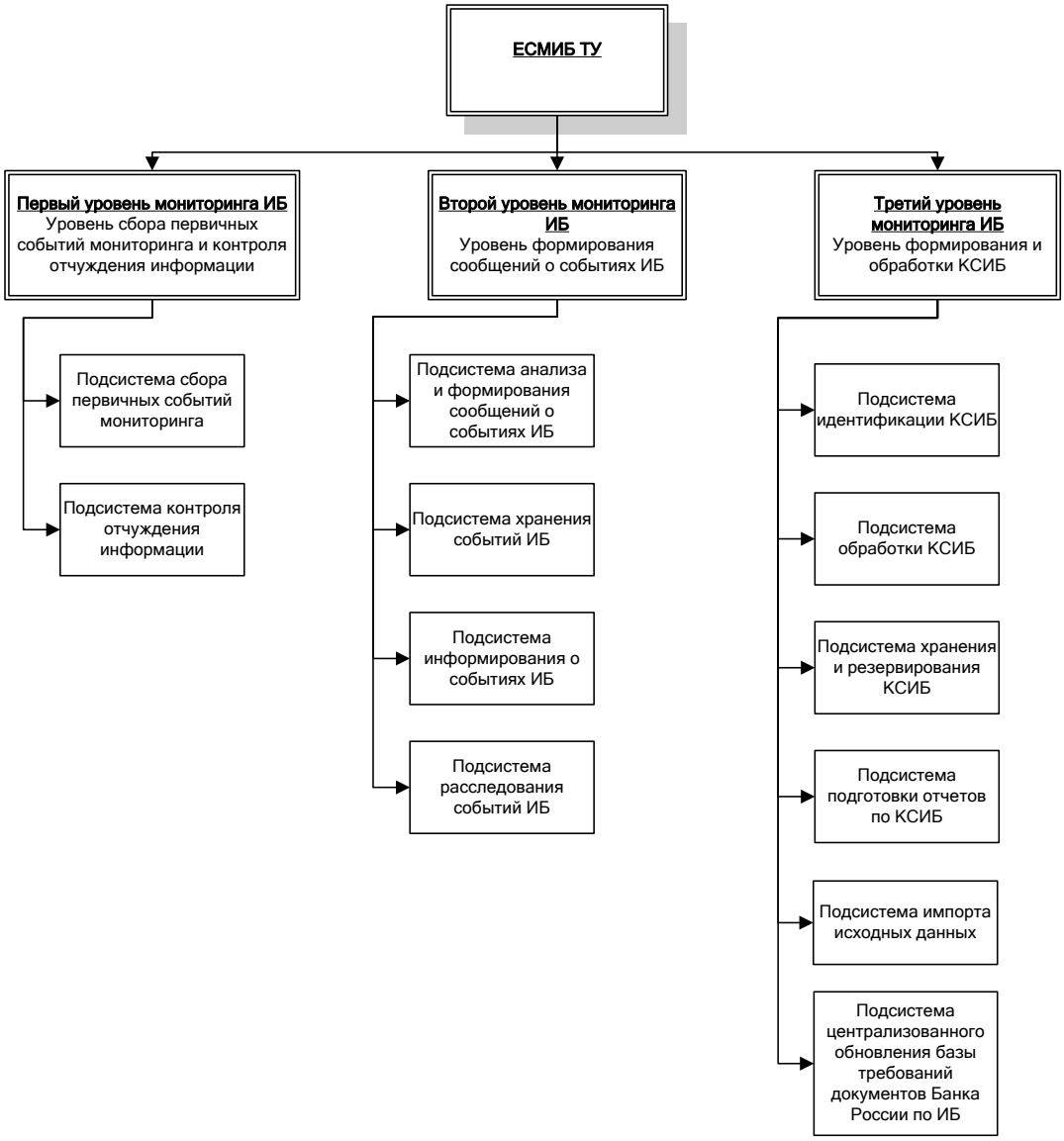

Рис. 5. 3. Конфигурация ЕСМИБ ТУ

Подсистема информирования предназначена для оперативного (в режиме, максимально возможно приближенном к режиму реального времени) графического представления персоналу ЕСМИБ ТУ результатов работы подсистемы анализа – информации о событиях ИБ.

Подсистема расследования предназначена для автоматизации деятельности персонала в части проведения отложенного анализа и генерации отчетов о событиях ИБ, содержащихся в подсистеме хранения событий ИБ.

Подсистема хранения событий ИБ предназначена для хранения результатов работы подсистемы анализа в БД событий ИБ ЕСМИБ ТУ.

Подсистема идентификации КСИБ предназначена для выявления КСИБ на основе правил анализа событий ИБ от разнотипных источников данных мониторинга объекта автоматизации с указанием нарушений требований

нормативных и иных актов Банка России по ИБ, а также передачи КСИБ в подсистему обработки. Подсистема идентификации КСИБ включает в свой состав средства для создания, редактирования, проверки и графического представления правил анализа событий ИБ (сценариев).

Подсистема импорта исходных данных предназначена для переноса информации из БД подсистемы хранения событий ИБ и получения данных о пользователях (сотрудниках ТУ) от АС ВХД для последующего использования в целях мониторинга ИБ.

Подсистема обработки КСИБ предназначена для регистрации, информирования, классификации по заданным критериям и фиксирования мер по устранению последствий КСИБ в соответствии с ролевыми функциями персонала ЕСМИБ ТУ.

Подсистема хранения и резервирования КСИБ предназначена для ведения оперативного архива и долговременного архива КСИБ, загрузки данных из долговременных архивов.

Подсистема подготовки отчетов по КСИБ предназначена для автоматизированной подготовки отчетов по КСИБ с учетом задаваемых параметров (временной интервал, оценка коррелированного события ИБ, его тип и т. п.), вывода на печать и экспорта в файл отчетов, а также просмотра отчетов и контроля настроек ЕСМИБ ТУ.

Подсистема централизованного обновления базы требований документов Банка России по ИБ.

Основной задачей первого уровня мониторинга ИБ в ЕСМИБ (рис.5.4) является сбор от подконтрольных объектов мониторинга и представление в унифицированном внутреннем формате информации о событиях мониторинга ИС. *Подконтрольный объект* - совокупность технических средств, системного и прикладного программного обеспечения, а также их персонала, получение информации о состоянии и действиях которых является необходимым условием обеспечения процесса мониторинга ИБ.

Состав подконтрольных объектов мониторинга определяется руководством исходя из значимости данных мониторинга ИБ для ИС организации.

Главный компонент первого уровня – *подсистема сбора первичных событий мониторинга* предназначена для автоматизированного сбора первичных событий мониторинга из журналов подконтрольных объектов ИС. В основу работы этой подсистемы положены следующие принципы:

– входными данными ЕСМИБ являются события мониторинга от разных источников, доставляемые собственными программными агентами;

– собственные программные агенты формируют события мониторинга, связанные с контролем устройств и съемных машинных носителей, а также ряд других событий, необходимых для анализа;

– на подконтрольные объекты не оказывается блокирующих воздействий;

– собственные программные агенты работают как непосредственно в среде подконтрольных объектов (т. е. локально), так и получают события

мониторинга удаленно, в зависимости от типа источника;

– результатом работы первого уровня мониторинга является набор событий мониторинга в унифицированном формате представления, не зависящем от типа источника.

Подсистема контроля отчуждения информации предназначена для фиксации первичных событий мониторинга о работе персонала ИС со съемными периферийными устройствами на подконтрольных объектах, работающих под управлением ОС Windows.

Рис. 5.4. Реализация первого уровня мониторинга ИБ в ЕСМИБ организации

Задачей второго уровня является формирование событий ИБ, их сохранение в базе данных, оперативное информирование персонала о зафиксированных событиях, обеспечение проведения расследования, т. е. поддержка запросов к базе данных, позволяющих установить контекст события ИБ: место, время, имя пользователя и прочее, а также сопутствующие события (рис. 5.5).

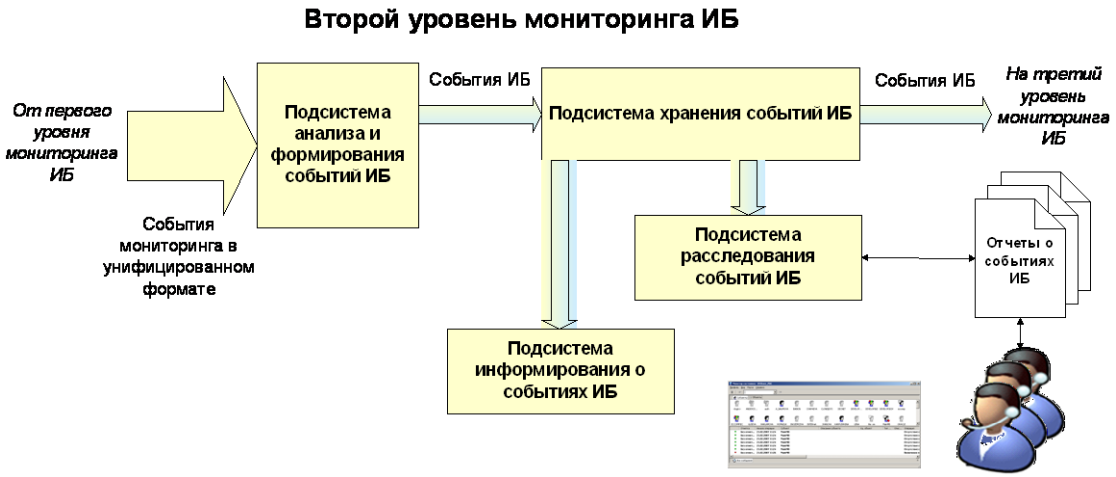

Рис.5.5. Реализация второго уровня мониторинга ИБ в ЕСМИБ организации

Основой второго уровня является *подсистема анализа и формирования событий ИБ*, предназначенная для автоматизированного анализа первичных событий мониторинга (входных данных) из журналов подконтрольных объектов ИС и формирования событий ИБ по заданным правилам с целью оценки степени их влияния на ИБ организации.

В зависимости от способа постановки используются два разных режима решения задачи: отложенный (для решения задач из перечня предопределенных) и оперативный (для решения сформулированных задач).

Отложенный режим решения предполагает применение соответствующего задаче *метода статистического анализа или метода выявления закономерностей* на массиве данных мониторинга ИБ, ограниченного заданными параметрами.

Структура процесса отложенного интегрального анализа приведена на рис. 5.6. Отложенный интегральный анализ реализуется над массивом исходных данных, образующимся в результате постановки задачи (статистической или выявления закономерностей), задания общих и специфичных для задачи набором параметров. По результатам решения поставленной задачи формируется заключение.

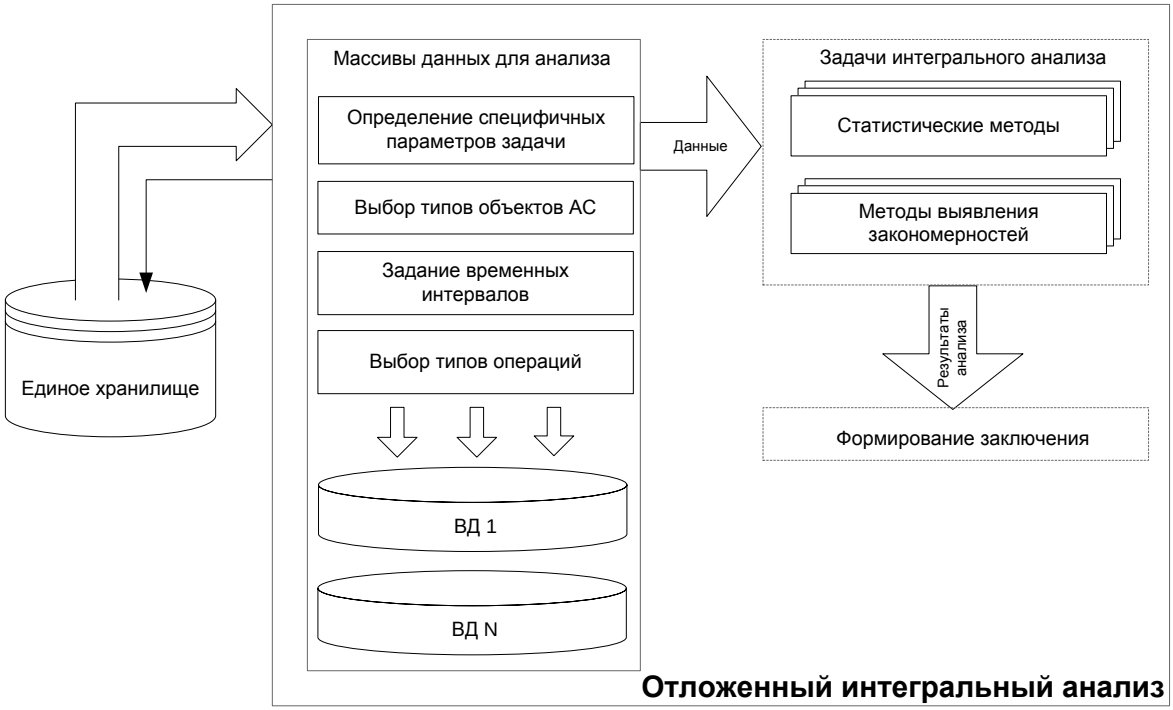

Рис. 5.6. Структура модуля отложенного интегрального анализа

Оперативный режим решения предполагает применение *сигнатурного анализа* упорядоченной, ограниченной параметрами последовательности операций, выполняемых в процессе функционирования ИС.

Общая схема *сигнатурного анализа* данных мониторинга второго уровня представлена на рис.5.7. Основные принципы функционирования подсистемы анализа:

– входными данными являются события мониторинга в унифицированном формате, сформированные подсистемой сбора;

– формирование событий ИБ осуществляется в соответствии с перечнем правил, описывающих штатную и нештатную работу пользователей и ПО объектов мониторинга;

– правила создаются в процессе настройки системы на основе общих положений документов ИБ регуляторов, политик по информационной безопасности для общесистемных продуктов и на основе опыта эксплуатации систем мониторинга ИБ в организации;

– результатом автоматизированного анализа событий мониторинга ИБ являются события ИБ. Объем событий ИБ существенно меньше объема событий мониторинга;

– автоматизированный анализ выполняется по мере поступления входных данных в режиме, максимально приближенном к режиму реального времени;

– события ИБ при формировании получают качественную оценку, используемую в отчетах о событиях ИБ по результатам расследований и при идентификации КСИБ на третьем уровне мониторинга ИБ.

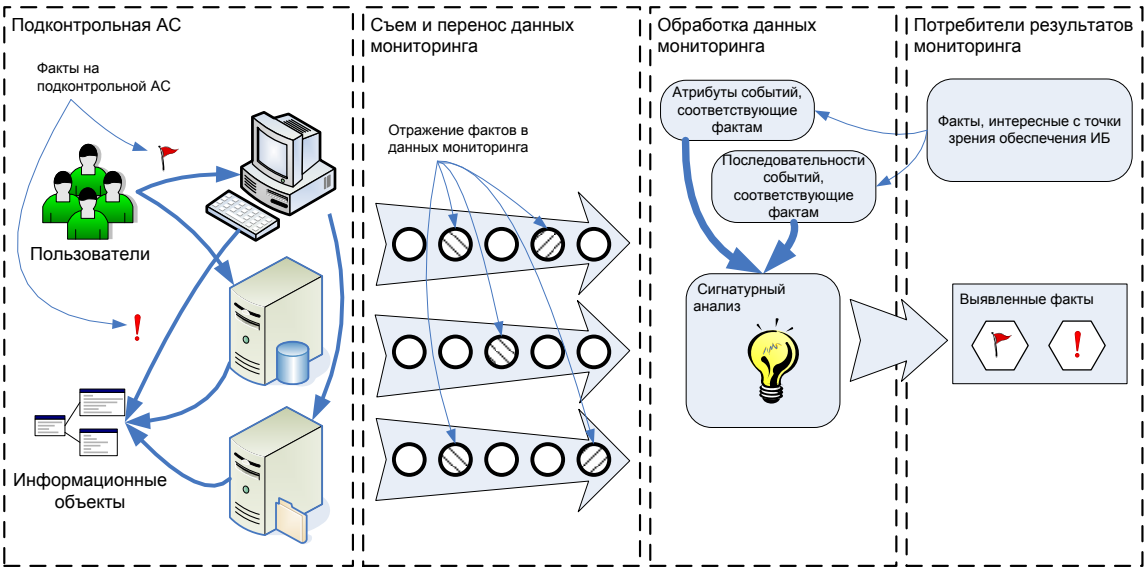

Рис. 5.7. Общая схема сигнатурного анализа

Перечень типов событий ИБ может насчитывать несколько сотен. Возможности ЕСМИБ по формированию *событий ИБ* в первую очередь определяются составом событий мониторинга, формируемых объектами наблюдения. От качества формирования событий мониторинга напрямую зависят и качество анализа и формирования событий ИБ.Примеры событий ИБ подсистемы анализа и формирования событий ИБ, являющиеся результатом работы второго уровня ЕСМИБ ТУ

– Вход/выход пользователя в систему/приложение.
– Запуск/завершение процессов.
– Работа с файлами (на локальных, сетевых и съемных носителях).
– Работа с объектами БД.
– Работа с информационными объектами в приложениях.
– Подключение/отключение периферийных устройств.
– Добавление/удаление СМН (компакт-диски, флэш-диски и др.).
– Отправление/прием почтовых сообщений и файлов.
– Работа по протоколам FTP и HTTP.
– Печать документов.
– Модификация информации реестра ОС Windows.

Подсистема хранения событий ИБ предназначена для хранения результатов работы подсистемы анализа в *базе данных (БД) событий ИБ*.

Подсистема информирования о событиях ИБ предназначена для оперативного (в режиме, приближенном к реальному времени) графического представления информации о событиях ИБ персоналу СОИБ.

Подсистема расследования событий ИБ предназначена для автоматизации деятельности персонала в части проведения отложенного анализа и генерации отчетов о событиях ИБ, содержащихся в подсистеме хранения.

Основными задачами третьего уровня ЕСМИБ (рис.5.8) являются идентификация и обработка коррелированных событий ИБ (КСИБ) .

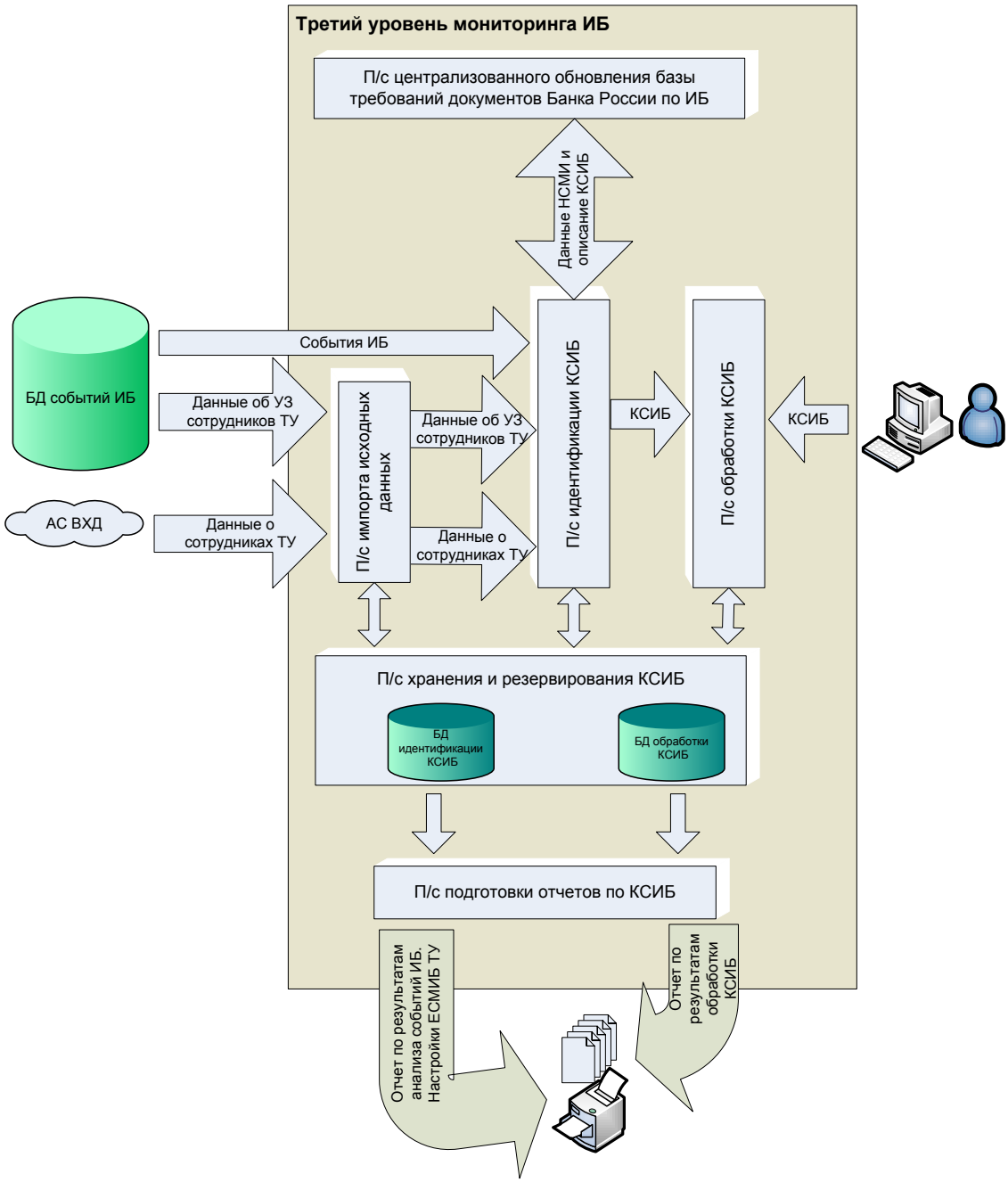

Рис. 5 .8.Реализация второго третьего уровня мониторинга ИБ в ЕСМИБ организации

КСИБ – это инцидент ИБ, выявленный *в результате сигнатурного анализа события ИБ или последовательности событий ИБ.* ЕСМИБ обеспечивает выявление КСИБ в результате автоматизированного анализа событий ИБ на наличие признаков неправомерных или подозрительных действий и/или операций, нарушающих требования нормативных документов ИБ организации и модели нарушителя. Анализ событий ИБ проводится как независимо для каждого объекта мониторинга, так и с учетом взаимных связей (корреляций) событий ИБ, зафиксированных для нескольких объектов мониторинга в составе ИС. При этом выявленный (идентифицированный) КСИБ характеризует реализацию угроз нарушения свойств ИБ задействованных информационных активов.

Подсистема идентификации коррелированных событий ИБ (рис. 5.9) предназначена для выявления КСИБ на основе правил анализа событий ИБ от разнотипных источников ИС с указанием нарушений требований нормативных документов организации по ИБ, а также передачи коррелированных событий ИБ в подсистему обработки. Подсистема идентификации должна включать в свой состав средства для создания, редактирования, проверки и графического представления правил анализа событий ИБ (сценариев).

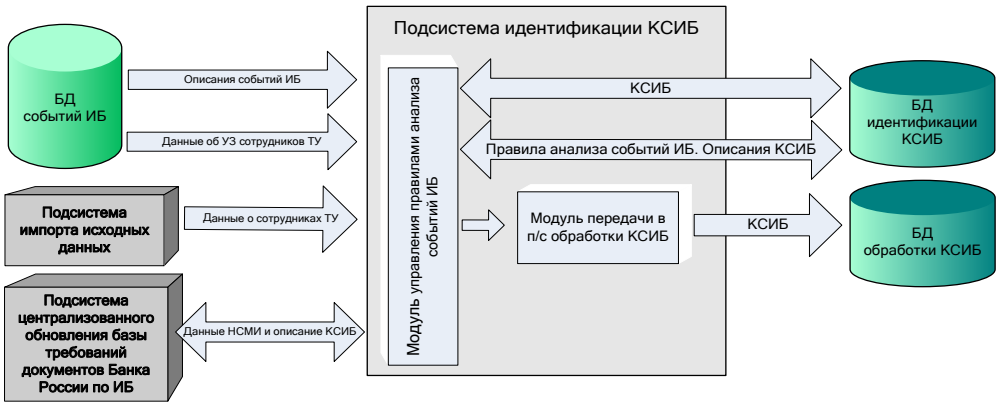

Рис. 5.9. Реализация третьего уровня мониторинга. Подсистема идентификации коррелированных событий ИБ

Основные принципы функционирования подсистемы идентификации:

– входными данными являются *события ИБ,сформированные подсистемой анализа и формирования событий ИБ второго уровня*;

– формирование (идентификация) КСИБ осуществляется в результате взаимоувязанного анализа событий ИБ от разных объектов мониторинга в соответствии с набором правил анализа, сформированных с учетом требований документов ИБ организации;

– идентификация может выполняться как по мере поступления входных данных в режиме, максимально приближенном к режиму реального времени, так и в отложенном режиме, по запросам персонала;

– каждое идентифицированное КСИБ содержит ссылку на нарушение конкретных требований нормативных документов ИБ организации и передается в подсистему обработки.

Интегральный анализ предполагает проведение совместной обработки разнородных данных мониторинга ИБ, полученных от различных ОС, СУБД и технических средств, функционирующих в составе ИС. На (рис. 5.10) показано изменение объема данных в процессе выполнения отдельных этапов интегрального анализа, обусловленное введением концепции конкретизации и дальнейшего уточнения целей анализа.

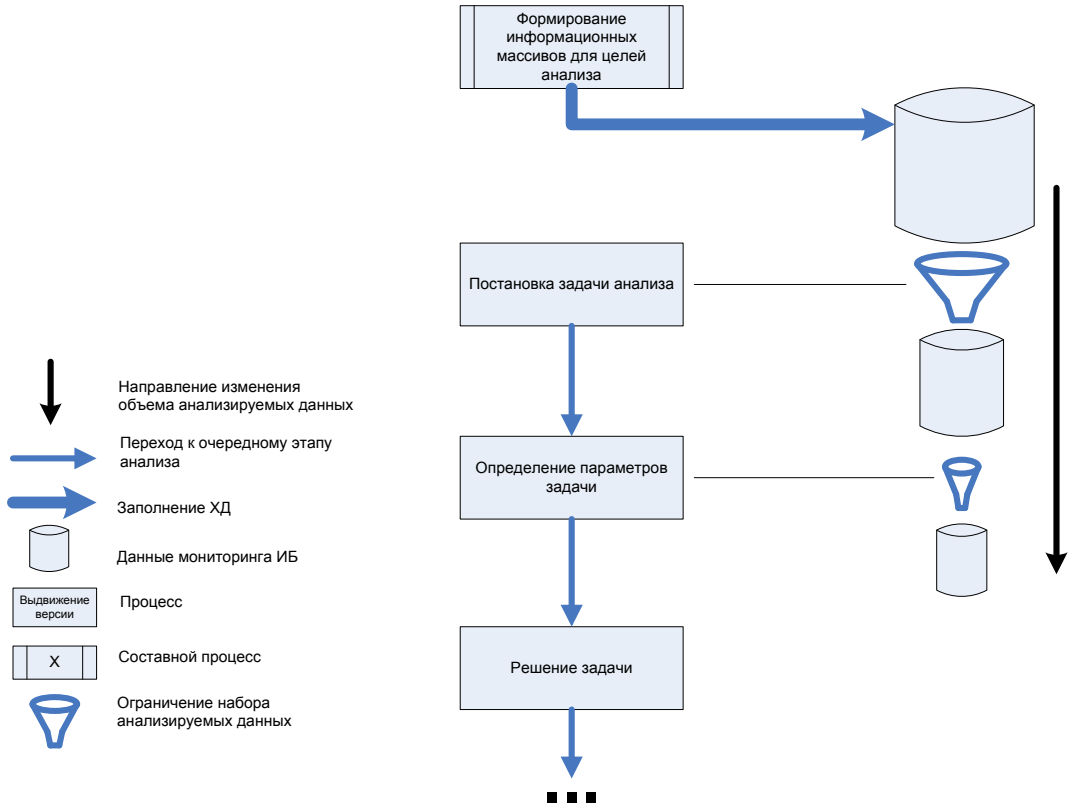

Рис.5.10. Изменение объема анализируемых данных в процессе интегрального анализа

Параметры задач однозначно определяются природой анализируемых данных. К числу источников данных значимых для целей интегрального анализа ИБ относятся:

– материалы по фактам обнаружения признаков нарушений, имеющих место в процессе использования разнородных критических ресурсов организации;

– сообщения лиц, имеющих прямой доступ к информации, относящейся к фактам нарушений;

– материалы ведущихся расследований;

– результаты анализа инцидентов по материалам завершенных расследований;

– открытые источники: анализ и обобщение информации, уже собранной правительственными и иными учреждениями, в том числе опубликованной в общедоступных документах;

– соответствующие положения нормативно-методических документов организации, описывающие порядок проведения интегрального анализа.

Общая схема выполнения методики интегрального анализа приведена на рис.5.11.

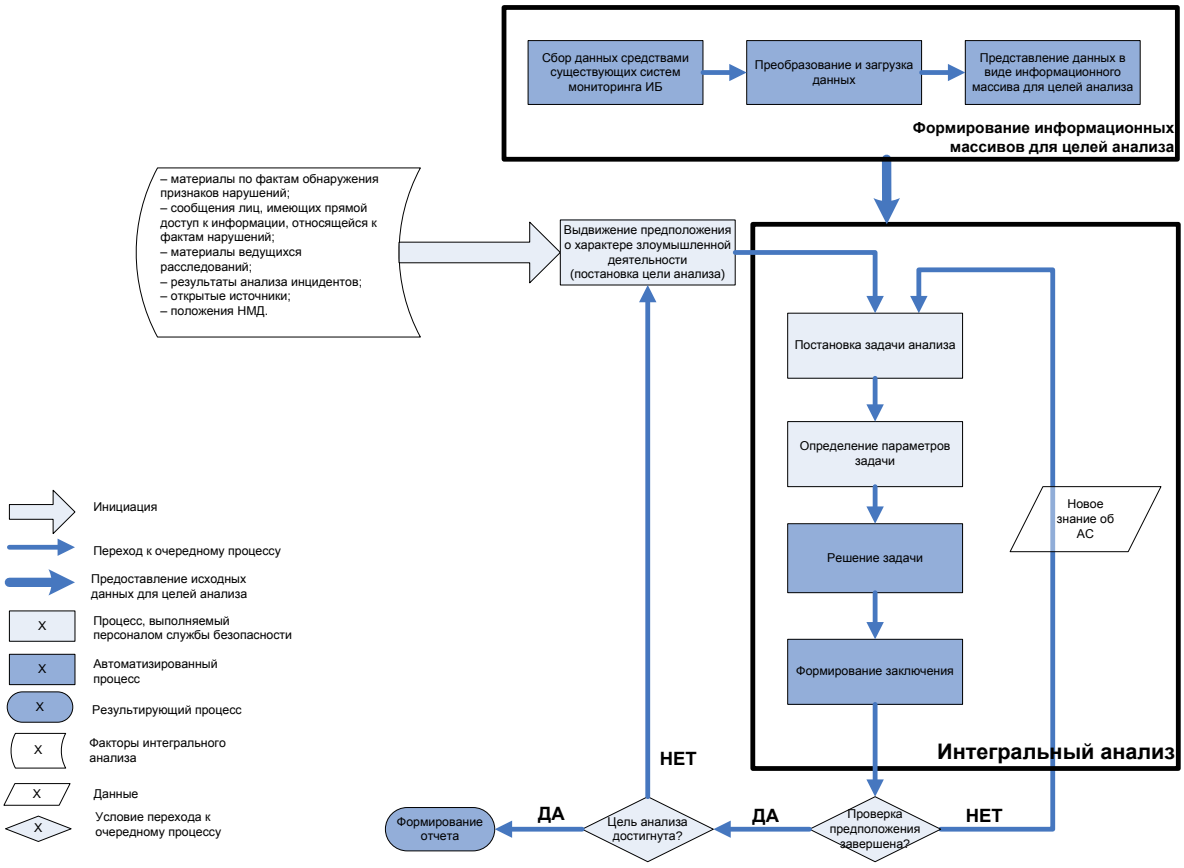

Рис.5.11. Общая схема выполнения методики интегрального анализа

Формирование информационных массивов для целей анализа (рис. 5.11) в общем случае является автоматизированным непрерывным процессом, выполнение которого поддерживается системой мониторинга ИБ.

Укажем основные особенности *подсистемы идентификации и коррелированного анализа ЕСМИБ*

– возможность одновременного анализа событий от нескольких разнородных источников (анализ событий ИБ проводится как независимо для каждого объекта мониторинга, так и с учетом корреляций событий ИБ: взаимных связей по пользователям, ресурсам, времени и пр. информационным параметрам событий ИБ);

– выявление незавершенных последовательностей;

– выявление циклических появлений событий в последовательности;

– использование при анализе возможности объединения нескольких учетных записей в одну карточку пользователя;

– возможность использования нескольких описаний последовательностей в контексте одного правила;

– декларативное описание правила анализа без использования элементов программирования;

– возможность ручной и автоматической регистрации КСИБ в подсистеме обработки;

– возможность регистрации КСИБ в любом узле описания последовательности.

Ввод исходных данных в подсистему импорта исходных данных происходит с целью использования в процессе взаимоувязанного анализа событий ИБ данных о сотрудниках организации и данных об их учетных записях.

Подсистема обработки КСИБ (рис. 5.12) должна обеспечивать реализацию функций регистрации, информирования, классификации по заданным критериям, и фиксирования мер по устранению последствий КСИБ в соответствии с ролевыми функциями персонала СОИБ.

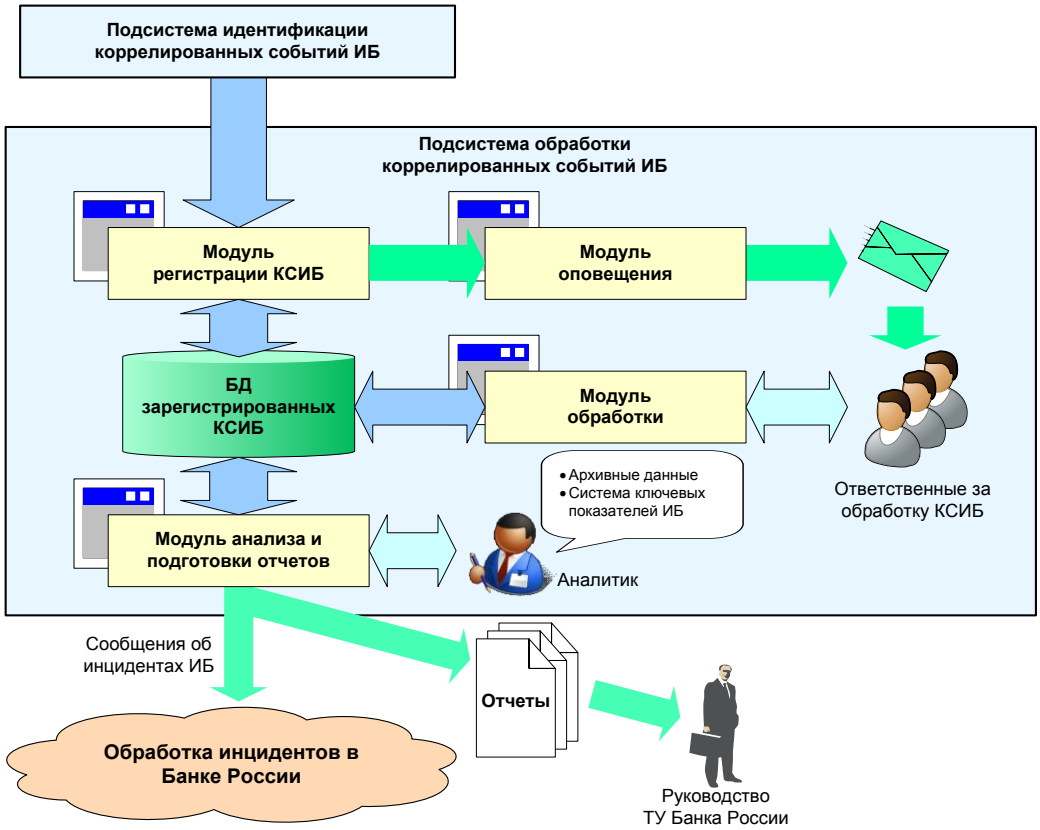

Рис.5.12. Третий уровень мониторинга. Подсистема обработки коррелированных событий ИБ в ЕСМИБ

Подсистема обработки КСИБ функционирует в соответствии со следующими принципами:

– входными данными являются КСИБ, сформированные подсистемой идентификации, либо зарегистрированные Регистратором посредством ввода информации в специализированную форму;

– подсистема обработки КСИБ обеспечивает последовательность обработки в соответствии с назначенными ролями персонала (Регистратор, Ответственный, Руководитель и др.). В зависимости от назначенной роли, персоналу доступны различные функции по обработке коррелированных событий ИБ. Например, разрешение (закрытие) коррелированного события ИБ может выполнить только пользователь с ролью «Ответственный» и т. д.;

– использование Web-технологий позволяет подключать новых ответственных лиц без установки дополнительного программного

обеспечения на их рабочие места. Доступ осуществляется по http-протоколу из Интернет-браузера, что предоставляет возможность работы с системой, не привязываясь к определенному рабочему месту.

Общая схема обработки коррелированных событий ИБ в ЕСМИБ приведена на рис.5.13.

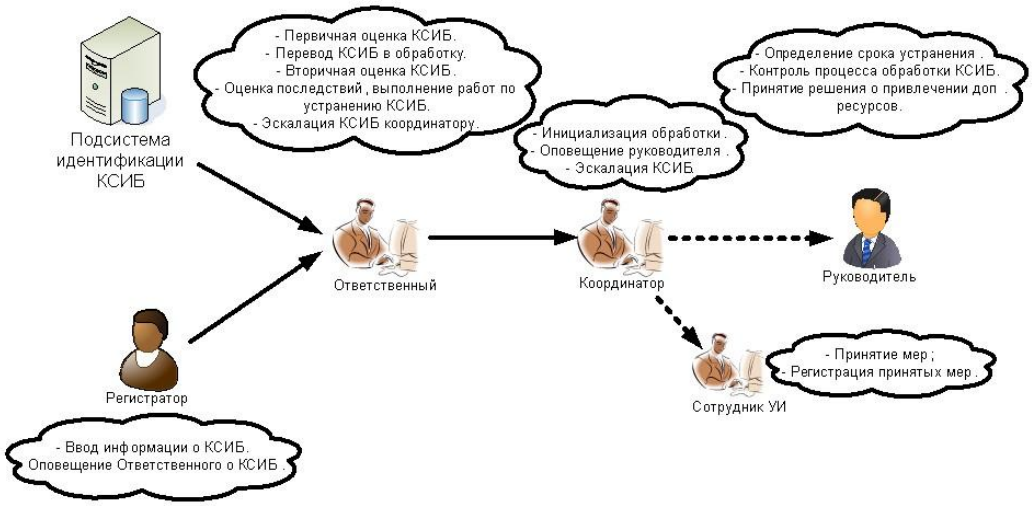

Рис.5.12. Общая схема обработки коррелированных событий ИБ в ЕСМИБ

В оперативном режиме выполняется анализ событий ИБ из нескольких источников одновременно без переписывания данных в промежуточное хранилище, с сохранением специфики и уникальности информации об источниках данных.

Подсистема хранения и резервирования коррелированных событий ИБ должна обеспечивать реализацию функций по ведению оперативного архива (например, в течение 30 дней) и долговременного архива (перенос данных, с освобождением дискового пространства, на отчуждаемые носители), загрузки данных из долговременных архивов.

Подсистема подготовки отчетов по коррелированным событиям ИБ должна обеспечивать реализацию функции автоматизированной подготовки отчетов по коррелированным событиям ИБ с учетом задаваемых параметров (временной интервал, оценка коррелированного события ИБ, его тип и т. п.), выводу на печать и экспорту в файл отчетов.

Структурная схема применения ЕСМИБ приведена на рис.5.14.

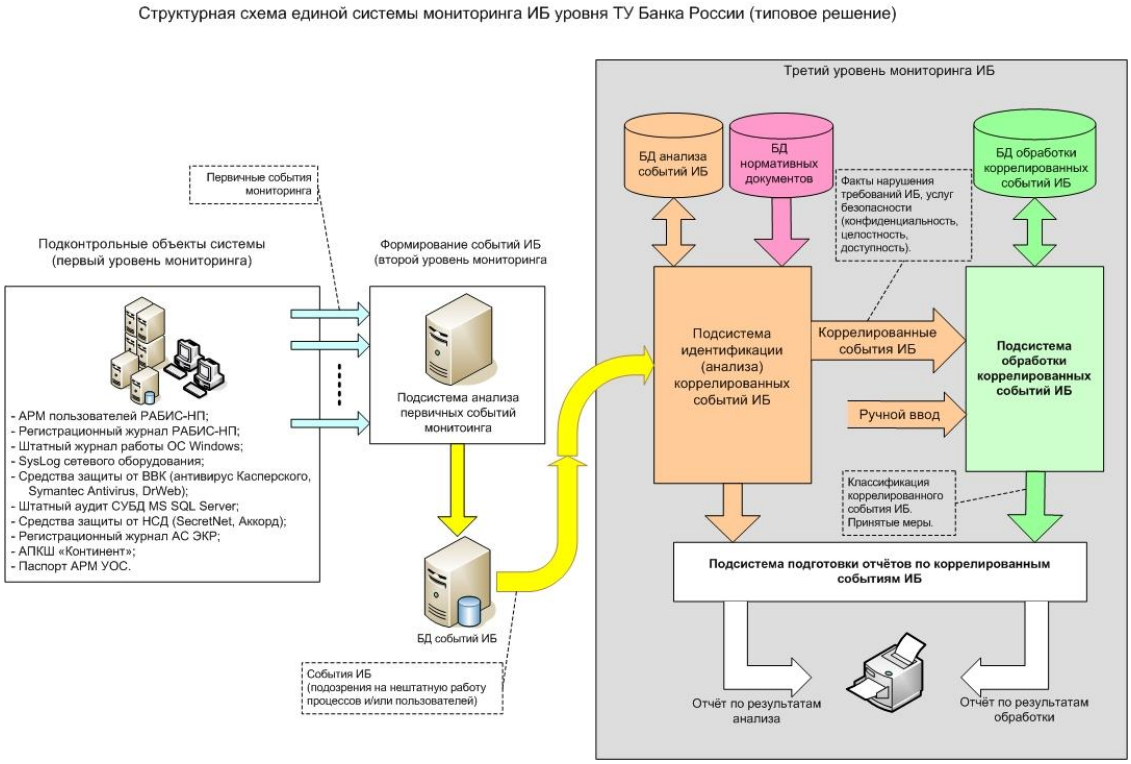

Рис.5.14. Структурная схема применения ЕСМИБ

5.3.4.Внедрение системы «Анализ функционирования СОИБ»

Для реализации система «Анализ функционирования СОИБ»должны быть внедрены следующие подсистемы:

– подсистема анализа соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации, требованиям законодательства Российской Федерации;

– подсистема анализа соответствия внутренних документов, требованиям Политик ИБ организации;

– подсистема оценки адекватности модели угроз организации существующим угрозам ИБ;

– подсистема оценки рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска;

– подсистема проверки адекватности используемых защитных мер требованиям внутренних документов организации и результатам оценки рисков;

– подсистема анализа отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

5.3.5. Внедрение системы «Обеспечение непрерывности бизнеса»

Система «Обеспечение непрерывности бизнеса»должна включать в себя следующие подсистемы:

– подсистемареагирования на инцидент и восстановления непрерывности бизнеса;

– подсистемаоценки результатов реагирования и оценки ущерба от инцидентов ИБ;

– подсистемаактивизации плана непрерывности бизнеса;

– подсистематестирования и проверки плана обеспечения непрерывности бизнеса;

– подсистема учета обучения и повышения осведомленности работников организации;

– подсистемаучета обязанностей работников по выполнению плана непрерывности бизнеса.

5.3.6. Документированные процедуры СУИБ для ввода в эксплуатацию

Документированные процедуры являются обязательным элементом *эксплуатации* СУИБ организации. Следовательно, в рамках системы управления необходимо разработать базу нормативных документов, описывающих все процедуры в области ИБ.

Основными документами по управлению ИБ являются *Политика управления информационной безопасностью* и *Политика информационной безопасности (Политика)*. Политика управления ИБ описывает общий подход к управлению ИБ. Кроме этого, разрабатываются методики и инструкции, описывающие *процедуры обеспечения ИБ и управления ею*. В качестве примеров можно привести следующие методики:

– Методика инвентаризации активов;

– Методика категорирования активов;

– Методика оценки информационных рисков;

– Методика обработки информационных рисков.

Инструкции следует разработать для каждой процедуры обеспечения информационной безопасности. Примерный перечень может содержать следующие инструкции:

– Инструкция по обеспечению сохранности конфиденциальной информации (соглашение о конфиденциальности);

– Инструкция пользователя по обеспечению информационной безопасности;

– Инструкция системного администратора по обеспечению информационной безопасности;

– Инструкция администратора безопасности;

– Инструкция по управлению доступом пользователей к информационной системе;

– Инструкция по защите от вредоносного программного обеспечения;

– Инструкция по выполнению резервного копирования;

– Инструкция по обращению со съемными носителями информации;

– Инструкция по использованию мобильных компьютеров;

– Инструкция по использованию средств криптографической защиты информации;

– Инструкция по внесению изменений в информационную систему;

– Инструкция по управлению инцидентами информационной безопасности;

– План непрерывности ведения бизнеса;

– Регламент обеспечения физической безопасности и др.

Как правило, на этапе «ВНЕДРЕНИЕ» СУИБ разрабатывают также *«План внедрения системы управления»*, в котором описывают четкую последовательность действий при внедрении процедур, методы контроля и осуществления проверок выполнения процедуры. Модель СУИБ формализуется в едином комплексе нормативных документов. В этот комплекс входят следующие основные документы:

– Концепция обеспечения ИБ;

– Политика информационной безопасности;

– Положение об информационной безопасности организации;

– План обеспечения непрерывной работы и восстановления работоспособности информационной системы в кризисных ситуациях;

– Правила работы с защищаемой информацией;

– Журнал учета нештатных ситуаций;

– План защиты информационных систем организации;

– Положение о правах доступа к информации;

– Инструкция по внесению изменений в списки пользователей и наделению пользователей полномочиями доступа к информационным ресурсам организации;

– Инструкция по внесению изменений в состав и конфигурацию технических и программных средств информационных систем;

– Инструкция по работе сотрудников в сети Интернет;

– Инструкция по организации парольной защиты;

– Инструкция по организации антивирусной защиты;

– Инструкция пользователю информационных систем по соблюдению режима информационной безопасности;

– Инструкция администратора безопасности сети;

– Аналитический отчет о проведенной проверке системы информационной безопасности;

– Требования к процессу разработки программного продукта;

– Положение о распределении прав доступа пользователей информационных систем;

– Положение по учету, хранению и использованию носителей ключевой информации;

– План обеспечения непрерывности работы организации (непрерывности ведения бизнеса);

– Положение по резервному копированию информации;

– Методика проведения полного анализа и управления рисками, связанными с нарушениями информационной безопасности.

Датой ввода СУИБ в эксплуатацию является дата утверждения высшим руководством организации Положения о применимости средств управления. Данный документ является публичным и декларирует цели и средства, выбранные организацией для управления рисками.

СУИБ организации можно считать внедренной и эффективнофункционирующейнапрактикетогда,когдавсеепроцедурыхотябы одинразпройдутэтапымоделиPDCA,когдабудутнайденыирешеныпроблемы,возникающие при внедрениипроцедур.

Обеспечение ИБ и управление ею – достаточно трудоемкие процессы. Однако если к ним подойти комплексно и своевременно, а также выполнять все рекомендации международных стандартов в области управления ИБ – ISO/IEC 27001:2005 и ISO/IEC 17799:2005, они станут прозрачными, а защита от угроз безопасности эффективной.

5.3.7. Подготовка СУИБ к сертификационному аудиту

На данном этапе организации рекомендуется пройти предварительный аудит, который поможет оценить готовность к сертификационному аудиту. Предварительный аудит обычно проводится тем же органом по сертификации, в котором предполагается прохождение сертификационного аудита. По результатам предварительного аудита орган по сертификации составляет отчет, в нем отмечаются все положительные стороны созданной СУИБ, выявленные несоответствия и рекомендации по их устранению.

Для проведения сертификационного аудита рекомендуется, чтобы СУИБ организации функционировала от трех до шести месяцев. Это минимальный период, необходимый для первичного выполнения внутренних аудитов и анализа СУИБ со стороны руководства, а также для формирования записей по результатам выполнения всех процедур СУИБ, которые анализируются в ходе сертификационного аудита.

Результатом данного этапа является СУИБ организации, подготовленная к прохождению сертификационного аудита.

5.4. Этап «ПРОВЕРКА» СОИБ

Задачей выполнения деятельности в рамках группы процессов «ПРОВЕРКА» СОИБ является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ. В рамках выполнения процессов этапа «ПРОВЕРКА» СОИБ предусматривается проведение следующих основных работ:

– мониторинг ИБ и контроль защитных мер;

– самооценка ИБ;

– аудит ИБ;

– анализ функционирования СОИБ (в том числе со стороны руководства).

Результат выполнения деятельности на этапе «ПРОВЕРКА» СОИБ является основой для выполнения деятельности по совершенствованию СОИБ.

5.4.1. Мониторинг ИБ и контроль защитных мер

Основными целями мониторинга и контроля защитных мер в организации являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели:

– контроль за реализацией положений внутренних документов по обеспечению ИБ в организации;

– выявление нештатных, в том числе злоумышленных, действий в ИС организации;

– выявление инцидентов ИБ.

Проведение мониторинга ИБ и контроля защитных мер включает:

– контроль параметров конфигурации и настроек средств и механизмов защиты, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ;

– сбор и хранение информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию защитных мер;

– сбор и хранение информации обо всех инцидентах ИБ, выявленных в процессе мониторинга СОИБ и контроля защитных мер в базе данных инцидентов ИБ;

– регулярное проведение пересмотров процедуры мониторинга СОИБ и контроля защитных мер в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также инцидентов ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

Результаты мониторинга СОИБ и контроля защитных мер и Порядок выполнения процедур пересмотра должны документально фиксироваться.

В организации должны быть документально определены роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также пересмотром указанных процедур, и назначены ответственные за выполнение указанных ролей.

5.4.1.1. Организационно–техническая схема применения ЕСМИБ

Целью применения ЕСМИБ, является контроль состояния информационной безопасности ИС на основе интегрального оперативного анализа санкционированных и несанкционированных действий пользователей (как легальных, так и нелегальных) для принятия решения о наличии или отсутствии в их действиях угроз для нарушения доступности, целостности или конфиденциальности информации в ИС и выдачи рекомендаций по совершенствованию защитных мер.

Изначально ЕСМИБ настраивается на генерацию предупреждений о нарушении при обнаружении несанкционированного действия хотя бы в одном из журналов штатного аудита компоненты ИС. Цель АИБ и экспертной системы ЕСМИБ – определить характер, источник и последствия

выявленного нарушения при помощи анализа журналов штатного аудита компонент ИС, систем защиты информации и правил экспертной системы. По мере накопления экспертной системой сведений о нарушениях и пополнении базы знаний работа АИБ автоматизируется в большей степени.

Некоторые практики применения ЕСМИБ приведены на рис. 5.6. -5.8 [45,46]. На рис.5.6. приведена схема работы правила «Контроль заражения компьютера вирусом». Используются данные из регистрационных журналов ПО «Антивирус Касперского» и системы «Контроль использования периферийных устройств» (например, Device Lock). КСИБ, возникший в результате срабатывания данного правила содержит не только информацию о факте обнаружения вредоносного кода, но и информацию об его источнике (в том числе серийный номер носителя). Это позволяет значительно ускорить расследование по факту обнаружения вредоносного кода.

Рис.5.6. Примеры формирования коррелированных событий ИБ. Попытка заражения АРМ «открытого» контура вирусом

На рис. 5.7. приведена схема работы правила «Контроль активности учетных записей сотрудников, находящихся в отпуске». Используются данные из регистрационного журнала системы 1С и других источников, для которых фиксируются события «регистрации пользователя в системе».

В случае, если в период отпуска, сотрудник регистрируется в какой-либо из систем (идентификатор определяется по карточке сотрудника в ЕСМИБ), то формируется КСИБ.

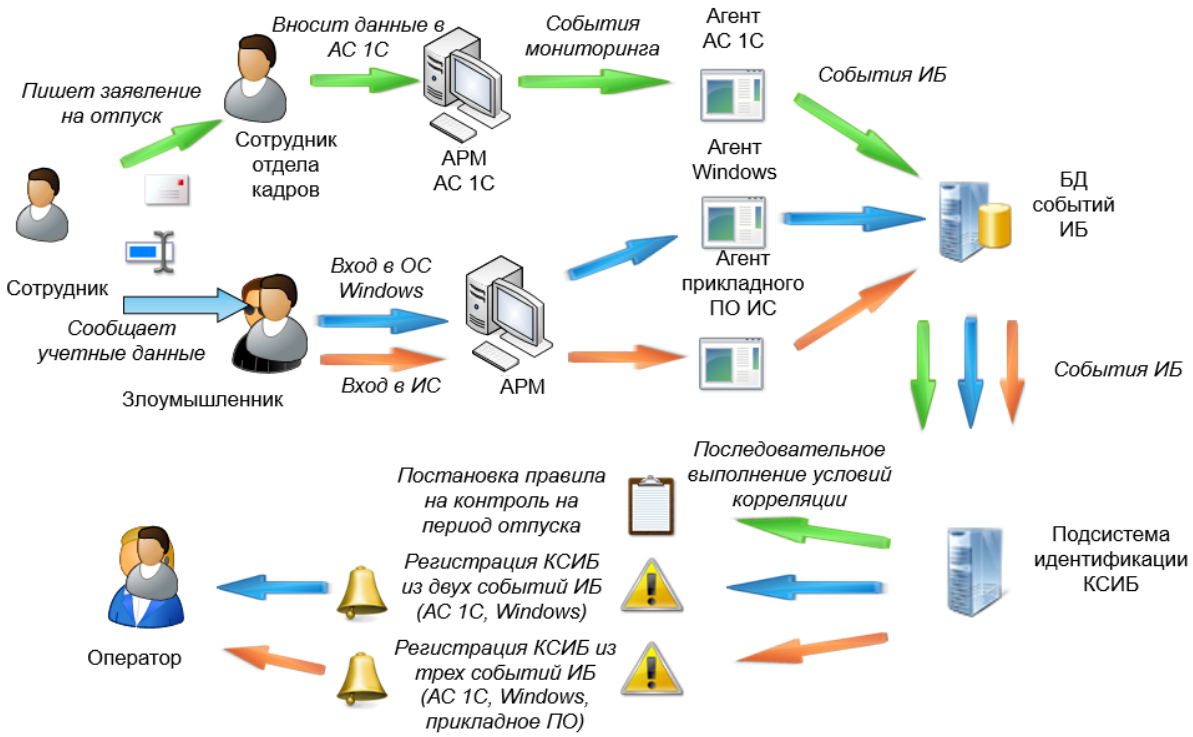

Рис.5.7. Примеры формирования коррелированных событий ИБ.Контроль активности учетных записей сотрудников «открытого» контура ИС, находящихся в отпуске

На рис.5.8. приведена схема работы правила «Контроль соответствия учетных записей Windows и 1С». КСИБ выявляет несоответствие учетных записей данного пользователя в операционной системе и 1С. Идентификаторы пользователя в операционной системе и 1С определяются по карточке пользователя. КСИБ возникает, когда пользователь воспользовался чужой учетной записью (возможно с иными полномочиями) в ОС или 1С.

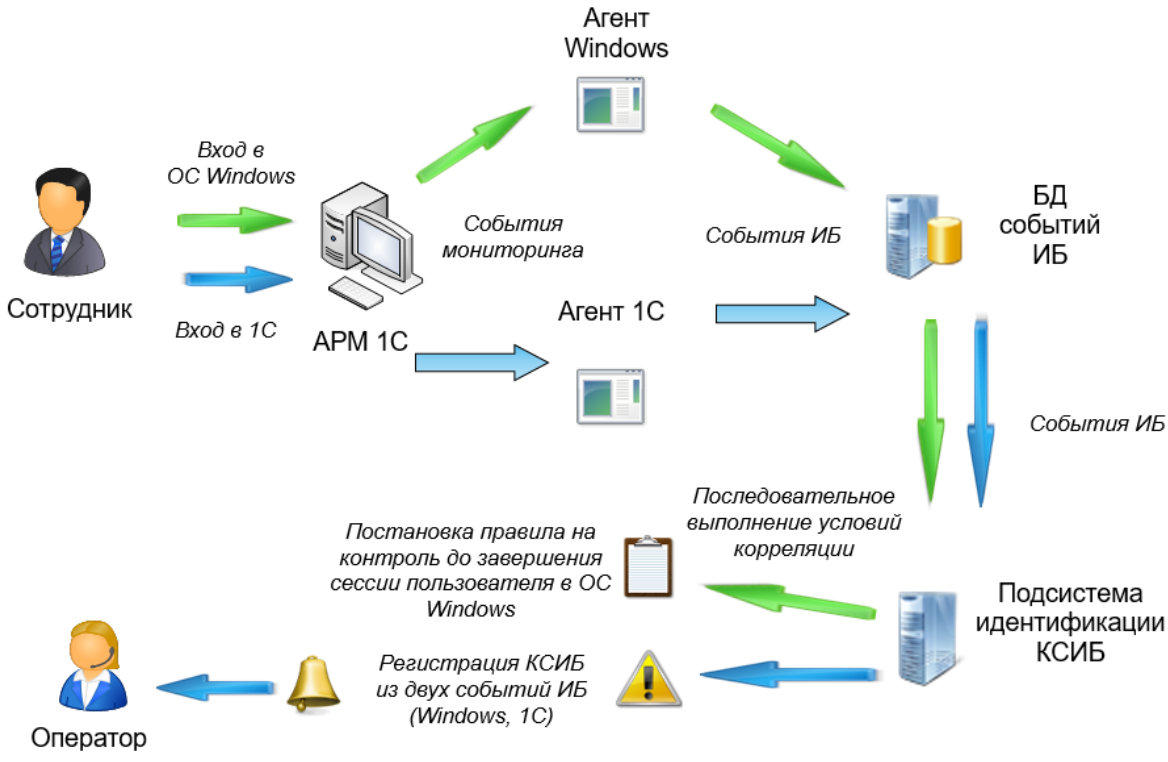

Рис.5.8.Примеры формирования коррелированных событий ИБ. Контроль соответствия учетных записей Windows и 1С «открытого» контура

Конкретная последовательность действий экспертов ЕСМИБ определятся характером обнаруженного нарушения или подозрительного действия и местом его обнаружения. Приведем примерную схему контроля состояния информационной безопасности в корпоративной сети и на серверах СУБД, ОСUnix

Для корпоративной сети:

– проанализировать журналы системы, где было обнаружено нарушение на предмет определения предыдущих событий в этой системе;

– изучив запись о нарушении, попытаться установить источник нарушения (локальный или удаленный). В случае локального нарушения, например, несанкционированного изменения правил фильтрации на маршрутизаторе Cisco, связаться с администратором системы для более детального расследования;

– в случае удаленного нарушения попытаться по цепочке с помощью исследования данных аудита других компонентов корпоративной сети идентифицировать источник нарушения;

– по результатам анализа провести корректировку настроек системы, где произошло нарушение с целью недопущения дальнейших нарушений;

– провести внеочередное тестирование компонент корпоративной сети с помощью сканера безопасности и реализовать полученный рекомендации по повышению уровня защищенности.

Для серверов СУБД, ОСUnix:

– проверить журналы аудита СУБД на наличие записей «действие пользователя с несанкционированным набором полномочий»;

– проверить журналы аудита СУБД на наличие записей «действие администратора СУБД по изменению полномочий».

В случае если изменения полномочий произведены без ведома администратора СУБД

– необходимо проверить журналы системы обнаружения вторжений с целью обнаружения удаленной атаки на СУБД, а также предпринять внеочередное тестирование СУБД с помощью сканнера безопасности;

– проверить ОС Unix средствами системных и сетевых сканеров безопасности на наличие изъянов в системе защиты ОС;

– проверить журналы аудита ОС Unix для обнаружения несанкционированных действий по изменению служебной информации ОС;

– проверить журналы аудита маршрутизаторов и межсетевых экранов с целью обнаружения попыток доступа к ресурсам центра обработки данных с использованием несанкционированных IP–адресов.

По результатам проверки по каждому из вышеуказанных пунктов АИБ могут производиться дополнительные действия по детальному выяснению причин возникновения нарушений. Также после завершения расследования

необходимо произвести дополнительное обучение экспертной системы для автоматизации обнаружения подобных нарушений в дальнейшем.

АИБ должен получать необходимые сведения, касающиеся функционирования систем от администраторов этих систем, которые, в свою очередь, обязан предоставить такие сведения и обосновать произведенные операции, отражаемые в файлах аудита.

Итогом проводимой работы по анализу данных должны явиться сводные отчеты о выявленных нарушениях и предложения по улучшению системы защиты ИС, вырабатываемые при помощи генератора отчетов системы интегрального аудита при участии администратора информационной безопасности. Кроме того, должны выпускаться аналитические обзоры по функционированию ИС для руководства организации с описанием и обоснованием предложений по усовершенствованию технологии защиты информации и применяемых средств защиты ИС.

По результатам анализа данных мониторинга и аналитической работы подразделение безопасности может вырабатывать рекомендации разработчикам компонент ИС по увеличению уровня информационной безопасности этих компонент.

Предусматривается различный уровень детализации отчетов системы интегрального аудита, предназначенных для изучения экспертами подразделения безопасности, а также руководством организации (обобщение результатов работы системы интегрального аудита). Например, для подразделения безопасности может генерироваться отчет, содержащий следующие сведения:

– подробная статистика НСД и инцидентов с описанием места, времени, указанием объекта и субъекта аудита, подробной интерпретацией события по каждому из журналов аудита;

– рекомендации необходимой дополнительной настройки штатных и внешних систем защиты и параметров аудита;

– данные о текущем состоянии обучения экспертной системы;

– выдача статистических оценок работы пользователей, гистограмм по работе системы защиты.

Для руководства организации могут генерироваться следующие отчеты:

– оценка работы администраторов и пользователей ИС, основанная на статистическом анализе журналов аудита;

– общая статистика по НСД и сбоям в ИС;

– общая статистика по инцидентам ИБ;

– сводная оценка работы подразделений организации.

5.4.2. Самооценка информационной безопасности

Самооценка соответствия ИБ организации требованиям ПИБ и стандартов РФ проводится в первую очередь подразделениями технической защиты информации организации. Самооценка ИБ должна проводиться в соответствии

с нормативно-методическими документами организации и/или соответствующего ведомства.

5.4.3. Аудит информационной безопасности

Должна быть документально определена и реализовываться программа аудитов ИБ организации, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

В отличие от самостоятельной оценки аудит не проводится тем же персоналом, который участвует в процессах планирования, внедрения и эксплуатации СОИБ. Это необходимо для обеспечения разделения ответственностей. Аудит может проводиться отделом внутреннего аудита организации. Аудит информационной безопасности включает:

– проверку соответствия политике безопасности и реализация Планов по безопасности;

– проведение аудита безопасности ИТ–систем;

– определение и принятие мер несоответствующего использования ИТ–ресурсов;

– проверку аспектов безопасности в других видах ИТ–аудита.

Внешний аудит (проводится внешними аудиторами) необходим для определения независимой внешней оценки эффективности СОИБ. Проведение внешнего аудита также требуют заказчики и третьи стороны.

5.4.4. Анализ функционирования СОИБ

Анализ функционирования СОИБ базируется в том числе на:

– результатах мониторинга СОИБ и контроля защитных мер;

– сведениях об инцидентах ИБ;

– результатах проведения аудитов ИБ и самооценок ИБ;

– данных об угрозах, возможных нарушителях и уязвимостях ИБ;

– данных об изменениях внутри организации, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации;

– данных об изменениях вне организации, например, данные об изменениях в законодательстве РФ, изменениях в договорных обязательствах организации.

Анализ функционирования СОИБ должен охватывать следующие функциональные области:

– периодический, а по возможности, динамический контроль защищенности, обеспечивающий своевременное выявление появившихся уязвимостей, которые могут быть использованы для нанесения атак;

– обнаружение атак в режиме реального времени, позволяющее своевременно определить и локализовать попытки выполнения

несанкционированных действий и выявить факты несанкционированного воздействия на компьютерные ресурсы;

– централизованное и упреждающее управление, позволяющее на основе автоматизированной поддержки принятия решений, а также эффективного контроля над пользователями и ресурсами сети снизить количество ошибок администрирования и предпринять превентивные меры, не допускающие развития событий по наихудшему сценарию.

Контроль защищенности предполагает периодическое, а в некоторых случаях – динамическое, выполнение следующих базовых функций:

– проверку системы защиты на соответствие новым руководящим и нормативным документам в области информационно–компьютерной безопасности;

– контроль правил корректного использования средств защиты в зависимости от их состава и назначения;

– контроль целостности и подлинности компонентов системы защиты;

– контроль корректности модификации параметров конфигурирования системы защиты;

– динамическая регистрация данных о функционировании системы защиты, их анализ и уведомление ответственных лиц при нарушении правильности работы защитных средств;

– тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак;

– контроль работоспособности подсистем защиты при моделировании нарушений работоспособности отдельных элементов компьютерной сети;

– проверка на отсутствие ошибок администрирования и конфигурирования;

– анализ политики формирования и использования эталонной информации (ключей, паролей и др.);

– проверка на наличие своевременных обновлений программных средств;

– проверка на отсутствие программных закладок и вирусов.

Таким образом, контроль защищенности предполагает исследование проверяемых объектов для выявления в них «слабых мест» и обобщение полученных сведений, в том числе в виде отчета.

Проверка системы защиты на соответствие новым руководящим и нормативным документам в области ИБ ИС позволяет своевременно выявить недостатки в системе защиты на основе анализа передового опыта по систематизации предъявляемых к таким системам требований.

Контроль правил корректного использования средств защиты в зависимости от их состава и назначения состоит в периодическом контроле и пересмотре политики безопасности на ее административном и процедурном уровнях. При изменении структуры, технологических схем или условий функционирования компьютерной системы, как концепция защиты, так и детальные процедурные меры могут меняться, в особенности, конкретные

инструкции по информационно–компьютерной безопасности, относящиеся к администраторам и пользователям компьютерной системы.

Контроль целостности и подлинности компонентов системы защиты предполагает периодическое или динамическое выполнение следующих действий:

– контроль наличия требуемых резидентных компонентов системы защиты в оперативной памяти компьютера;

– контроль всех программ системы защиты, находящихся во внешней и оперативной памяти, на соответствие эталонным характеристикам;

– контроль корректности параметров настройки системы защиты, располагаемых как в оперативной, так и во внешней памяти;

– контроль корректности эталонной информации (идентификаторов, паролей, ключей шифрования и т.д.).

При контроле корректности модификации параметров конфигурирования системы защиты подсистема контроля не должна допустить установку параметров, противоречащих политике безопасности, принятой в организации.

Регистрация данных о функционировании системы защиты предполагает фиксацию и накопление информации о следующих действиях:

– действиях всех подсистем защиты;

– действиях всех администраторов и пользователей других категорий по использованию защитных средств.

Кроме регистрации данных о функционировании системы защиты должен быть обеспечен и периодический анализ накопленной информации. Основной задачей такого анализа является своевременное определение недопустимых действий, а также прогнозирование степени безопасности информации и процесса ее обработки в вычислительной системе.

Для возможности и результативности периодического анализа предварительно должны быть подготовлены правила, описывающие политику работы системы защиты по одному из принципов:

– в работе системы защиты допустимо все, что не запрещено;

– в работе системы защиты запрещено все, что явно недопустимо.

Более высокий уровень контроля и безопасности обеспечивает второй принцип, так как на практике не всегда удается полностью учесть все действия, которые запрещены. Надежнее определить все действия, которые разрешены, и запретить все остальные.

При обнаружении подсистемой контроля любых нарушений в правильности функционирования подсистемы защиты должно быть выполнено немедленное уведомление соответствующих представителей службы безопасности.

Тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак выполняется с помощью специализированных средств анализа защищенности, которые, как правило, обеспечивают выполнение и оставшихся функций контроля защищенности.

Результаты анализа функционирования СОИБ должны документироваться.

В организации должны быть документально определены роли, связанные с процедурами анализа функционирования СОИБ, и назначены ответственные за выполнение указанных ролей.

В организации должен быть определен и утвержден руководством *план выполнения деятельности по контролю и анализу СОИБ.* В частности, указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации.

5.4.5. Обеспечение проведения анализа СОИБ со стороны руководства организации

В организации должен быть утвержден перечень документов необходимых для проведения *анализа СОИБ и предоставляемых руководству,* В частности, в указанный перечень документов должны входить:

– отчеты с результатами мониторинга СОИБ и контроля защитных мер;

– отчеты с результатами анализа функционирования СОИБ с учетом выявленных уязвимостях и угрозах ИБ, а также выявленных инцидентах ИБ и др.

5.5. Этап «СОВЕРШЕНСТВОВАНИЕ» СОИБ

В связи с изменением рисков при изменениях в ИТ–инфраструктуре, в организации и в бизнес–процессах необходимо обеспечить должную поддержку мер безопасности. Поддержание эффективного функционирования системы безопасности проводится на этапе «СОВЕРШЕНСТВОВАНИЕ» СОИБ с учетом результатов мониторинга и анализа ИБ, полученных на этапе «ПРОВЕРКА» СОИБ.

Группа процессов на этапе «СОВЕРШЕНСТВОВАНИЕ» СОИБ включает в себя деятельность по принятию решений о реализации тактических и/или стратегических улучшений СОИБ. Указанная деятельность, т. е. переход к этапу «СОВЕРШЕНСТВОВАНИЕ», реализуется только тогда, когда выполнение процессов этапа «ПРОВЕРКА» СОИБ дало результат, требующий совершенствования СОИБ. При этом сама деятельность по совершенствованию СОИБ должна реализовываться в рамках групп процессов «РЕАЛИЗАЦИЯ» и при необходимости — «ПЛАНИРОВАНИЕ». Пример первой ситуации — введение в действие существующего плана обеспечения непрерывности бизнеса, поскольку на стадии «Мониторинг ИБ и защитных мер» этапа «ПРОВЕРКА» СОИБ определена необходимость в этом. Пример второй ситуации — идентификация новой угрозы и последующие обновления оценки рисков на стадии «ПЛАНИРОВАНИЕ». При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СОИБ и при необходимости проводилось соответствующее обучение.

Целями процесса «СОВЕРШЕНСТВОВАНИЕ» являются

– улучшение соглашений в отношении информационной безопасности;
– совершенствование средств и контролей информационной безопасности.

В рамках процесса «СОВЕРШЕНСТВОВАНИЕ» СОИБ проводится:
– оценка новых угроз и уязвимостей ИБ;
– анализ оценок функционирования СОИБ со стороны руководства;
– актуализация базы данных успешных практик в области ИБ (собственных или других организаций);
– актуализация базы данных изменений: в законодательстве РФ; нормативных актах организации; интересах, целях и задачах бизнеса.

5.5.1. Направления совершенствования СОИБ в виде корректирующих или превентивных действий в плане тактических улучшений

Решения по тактическим совершенствованиям СОИБ как правило затрагивают корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ организации и не требующие пересмотра политики ИБ.

5.5.2. Направления совершенствований СОИБ в виде корректирующих или превентивных действий в плане стратегических улучшений

Решения по стратегическим совершенствованиям СОИБ затрагивают корректирующие или превентивные действия, связанные с пересмотром политики с последующим выполнением соответствующих тактических улучшений СОИБ, и указывают направления стратегических совершенствований:
– уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ организации;
– изменение в области действия СОИБ;
– уточнение описи типов информационных активов;
– пересмотр моделей угроз и нарушителей;
– изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

В случаях принятия решений по тактическим и стратегическим совершенствованиям СОИБ должны быть назначены ответственные за их реализацию.

Контрольные вопросы по гл. 5

1. Сформулируйте определение «информационная безопасность» в широком и узком смысле. Сформулируйте назначение системы управления ИБ организации.
2. На каких методических рекомендациях и стандартах базируется процессный подход к построению систем управления ИБ?
3. Опишите модель Деминга — модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью. Приведите этапы жизненного цикла системы управления информационной безопасностью организации.

4. Какие два основных принципа управления декларирует Стандарт ISO 27001?

5. Какие процедуры должны выполняться на этапе «Планирование» СОИБ?

6. Какие процедуры должны выполняться на этапе «Внедрение» СОИБ?

7. Какие процедуры СУИБ должны выполняться на этапе «Проверка» СОИБ?

8. Какие процедуры должны выполняться на этапе «Совершенствование» СОИБ?

9. Планирование системы ИБ. Определение политики ИБ. Этапы создания ПИБ.

10. Какие работы проводятся в процессе анализа рисков? Категорирование активов организации (идентификация всех активов в рамках выбранной области деятельности, определение ценности идентифицированных активов)

11. Оценка защищенности информационной системы организации (идентификация угроз и уязвимостей для идентифицированных активов). Угроза, уязвимость, обвал, инцидент, ущерб

12. Модель угроз. Значимые угрозы. Атака. Меры обеспечения информационной безопасности

13. Оценка информационных рисков. Основные методики оценки рисков информационной безопасности

14. Обработка информационных рисков (выбор критериев принятия рисков). План обработки рисков. Методика проведения анализа риска

15. Планирование системы мониторинга СОИБ и контроля защитных мер

16. Планирование системы самооценки, аудита, контроля и анализа, а также системы непрерывности бизнеса организации СОИБ организации.

17. Сформулируйте задачи этапа «Внедрение» СОИБ. Выбор защитных мер и механизмов защиты.

18. Внедрение процессов управления рисками. Какие два вида деятельности включает в себя управление рисками?

19. Количественные методики управления рисками. Методика управления рисками CRAMM и Методика RiskWatch. Качественные методики управления рисками. Методика управления рисками COBRA

20. Внедрение процессов управления инцидентами информационной безопасности. Проблемы управления инцидентами информационной безопасности. Способы борьбы с уязвимостями

21.Внедрение процедур системы мониторинга СОИБ и контроля защитных мер. Основные модели и принципы построения ЕСМИБ. Реализация ЕСМИБ

22. Внедрение системы «Анализ функционирования СОИБ». Внедрение типовой системы «Обеспечение непрерывности бизнеса»

23. Сформулируйте задачи этапа «ПРОВЕРКА» СОИБ

24. Мониторинг ИБ и контроль защитных мер. Организационно–техническая схема применения ЕСМИБ

25. Основные вопросы контроля проведения самооценки и аудита ИБ СОИБ

26. В чем состоит контроль проведения анализа функционирования СОИБ

27. Сформулируйте комплексный подход к поддержанию функционирования СОИБ в актуальном состоянии

28. Основные положения контроля СОИБ со стороны руководства организации

29. Какие цели и задачи процессов на этапе «Совершенствование» СОИБ?

30.Какие основные направления совершенствования СОИБ в виде корректирующих или превентивных действий в плане тактических и стратегических улучшений?

31. Какая база нормативныхдокументов должна быть разработана при подготовке к вводу в эксплуатацию СУИБ?

32. Какие работы проводятся при подготовке СУИБ к сертификации?

Заключение

Система защиты ИС должна строиться с учетом требований Политики информационной безопасности с учетом анализа риска, вероятностей реализации угроз безопасности и уязвимостей в конкретной ИС и обоснованного рационального уровня затрат на защиту.Требования к уровню защищенности активов ИС в конкретной предметной области должны устанавливаться (определяться) с учетом моделей нарушителей и угроз на основе анализа серьезности последствий нарушения базовых услуг безопасности: доступности, целостности и конфиденциальности.

Правильно построенная (адекватная реальности) модель нарушителя и угроз – важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Оценка вероятностей реализации угроз и наносимого ущерба сложна и возможна только с учетом особенностей конкретной системы обработки информации в целом. Экономическая сторона проблемы выбора средств защиты представляет собой оптимизационную задачу определения такого уровня затрат на создание системы защиты (такого уровня эффективности защиты) при котором вероятность нанесения ущерба определенного размера не превышала бы заданной величины.

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Они должны выступать в качестве обеспечения эффективного применения других методов и средств защиты в части касающейся регламентации действий людей с учетом того, что главную опасность для ИС представляет «человеческий фактор». Обязанности должностных лиц должны быть определены таким образом, чтобы при эффективной реализации ими своих функций обеспечивалось разделение их полномочий и ответственности.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности ИС и комплексном использовании определенных совокупностей различных мер защиты на всех этапах жизненного цикла системы начиная со стадий ее проектирования.

Вместе с тем обеспечение безопасности не может быть одноразовым. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких и слабых мест и потенциально возможных угроз ИС.

Приложение 1

Формализация процессов предоставления механизмов защиты в корпоративной мультисервисной сети. Общий подход

Известно [16,25-29,32,33,63-66], что любые механизмы защиты вносят временную, протокольную и потоковую избыточность в информационное окружение сети и приводят к ухудшению ее характеристик. Эти виды избыточности при проектировании защищенной корпоративной МСС должны быть учтены в ее критериях эффективности и ограничениях задач анализа [16,67-69]. Прикладные аспекты указанной проблемы связаны с повышением качества проектирования защищенных МСС, что в конечном итоге приводит к повышению эффективности использования сетевых ресурсов и сокращению затрат на их создание.

Ниже строятся модели процессов задействования специальных механизмов защиты. Метод оценки влияния механизмов защиты на информационное окружение ИТС, реализованной на технологии IP-QoS, базируется на общих принципах, разработанных и сформулированных в [69].

Задача анализа МСС. Пусть входная мультимедийная нагрузка по вызовам дается выражением $Y^{malty} = \left\| a_{ij}^{malty} \right\| = Y^B + Y^C = \left\| a_{ij}^B \right\| + \left\| a_{ij}^C \right\|$, где Y^C и Y^C – матрицы тяготений мультимедийной нагрузки (цифровая речь класса B и данные класса C в терминах ATM Fotum). Задача анализа МСС в общем виде формулируется следующим образом [16,67-69]. При заданной топологии МСС, структуре двухкомпонентных мультимедийных потоков Y^B и Y^C, заданной системе маршрутов $M_{st}^{B(C)}$ найти оптимальные значения длины речевых пакетов L_{opt}^B и значения коэффициентов загрузки ρ_{ij}^B, доставляющих максимум функционалу

$$\arg\max K^B\left(L^B, \rho_{ij}^B\right) \tag{2}$$

при ограничениях

$$\sum_{m=1}^{M_{st}^B} p_{st,m}^B \left(1 - F_{st,m}^B\left(\theta_{st}^B\right)\right) \le d^B,$$

$$L^B \lhd \theta_{st}^B \upsilon^B - H_{IP},$$

$$0 \le \rho_{ij}^B \lhd 1, \ \forall\, st \in S^B : a_{st}^B \ne 0. \tag{2}$$

По полученным значениям $\rho_{ij}^{B\max}$ и L_{opt}^B найти значения $\rho_{ij}^{C\max}$ и L_{opt}^C, доставляющих максимум функционалу

$$\arg\max K^C\left(L^B, \rho_{ij}^B, L^C, \rho_{ij}^C\right) \tag{3}$$

при ограничениях

$$T_{st}^C = \sum_{m=1}^{M_{st}^C} p_{st,m}^C \left(\sum_{ij \in l_{st,m}^{Cp}} T_{ij}^C + \sum_{\forall j: ij \in l_{st,m}^{Cp}} T_j^C \right) - \frac{L^C - H_{IP}}{\omega^C} \le T^C$$

или

$$\sum_{m=1}^{M_{st}^C} p_{st,m}^C \left(1 - F_{st,m}^C\left(\mathrm{T}^C\right)\right) \le d^C, \ \ \forall\, st \in S^C : a_{st}^C \ne 0 \tag{4}$$

и все параметры первой задачи найдены и фиксированы.

Здесь $p_{st,m}^{B(C)}$ – вероятность выбора m-го маршрута $l_{st,v}^{B(C)}$ из множества $M_{st}^{B(C)}$; $F_{st,m}^{B(C)}$ – функция распределения сквозного времени пребывания $\theta_{st}^{B}\left(T^{C}\right)$ речевого пакета (пакета данных) в тракте $st \in S^{B(C)}$. $d^{B(C)}$ – вероятность превышения задержки $\theta_{st}^{B}\left(T^{C}\right)$ пребывания пакетов в тракте передачи $st \in S^{B(C)}$. T_j^C – задержка пакетов в коммутационном поле маршрутизатора, с; T_{ij}^C – время обслуживанием пакетов в маршрутизаторе, с; $\left(L^C - H_{IP}\right)/\omega^C$ – время накопления информационной части пакета у отправителя, с (H_{IP} – длина заголовка *IP*-пакета, бит; ω^C – скорость работы установки данных в мультимедийной оконечной установке, бит/с); υ^B – скорость работы речепреобразующего устройстве в мультимедийной оконечной установке, бит/с.

Формализация процессов предоставления механизмов защиты. Предоставление механизмов защиты осуществляется по принципам предоставления сервиса базовой эталонной модели взаимодействия открытых систем [19,20]. Будем различать

1) *протокольные механизмы защиты*, применение которых преобразует структуру и/или формат уровневого примитива архитектуры МСС и вносит временную и/или протокольную избыточность в информационное окружение сети (например, механизмы симметричного шифрования с и механизмы обеспечения целостности с применением симметричных ЭЦП без центра сертификации (Authentication Center,*CA*); коды обнаружения целостности и/или имитозащитных вставок (ИЗВ)). При этом могут быть востребованы один или одновременно несколько механизмов защиты соответствующего логического уровня при формировании защищенного протокольного блока для каждого типа информации многокомпонентной потоковой структуры мультимедийного соединения в режиме сессии.

2) *потоковые механизмы защиты*, применение которых порождают дополнительный трафик безопасности и вносит потоковую избыточность в информационное окружение сети (например, механизмы защиты с применением простой аутентификации без защиты, «Заполнение трафика», «Нотаризация»). Кроме того, трафик безопасности порождается при обмене сертификатами центра сертификации *CA* между центром и корреспондентом в процессе аутентификации открытых ключей и формировании сеансовых ключей в двухключевых криптосистемах; при восстановлении целостности сообщений. Эти процессы включают в себя как фазу передачи сервисных примитивов трафика безопасности, так и процесс их обработки в оконечных системах.

3) *гибридные механизмы защиты*, применение которых как преобразует структуру и/или формат уровневого примитива, так и порождают дополнительный трафик безопасности (например, механизмы обеспечения целостности с применением ассиметричной ЭЦП, механизмы простой

аутентификации с защитой, механизмы строгой аутентификации и др.) Определим, что в первом случае процессы предоставления услуг безопасности моделируется системами массового обслуживания с протокольной услугой безопасности (СМОПб), во втором – отдельными однофазными или многофазными СМО с потоковой услугой безопасности (СМОУб), в третьем – сочетаниями указанных СМО.

Моделирование процессов предоставления протокольных механизмов защиты. Рассмотрим типовые модели процессов предоставления механизмов защиты, вносящих временную и протокольную избыточность в информационное окружение сети, на примерах механизмов «Шифрование» (предоставление криптографических процедур в одноключевой криптосистеме) и «Контроль целостности» (применение имитозащитных вставок).

Механизмы шифрования. Механизмы шифрования или криптографические механизмы представляют собой совокупность криптографических алгоритмов и крипто переменных секретных величин. Различают симметричные и ассиметричные системы шифрования или одно ключевые и двух ключевые шифры. Симметричные системы применяются в основном для предоставления криптографических процедур, в то время как применение асимметричных шифров можно свести к двум основным аспектам применения [69, 70]: 1) цифровая подпись $S^i(M)$, когда отправитель i«подписывает» сообщение M с помощью своего личного ключа S_i; 2) обмен ключами, при котором происходит обмен сеансовым ключом с применением личных ключей одной и/или обеих сторон.

Симметричное шифрование E (дешифрование D) базируется на централизованном изготовлении и распространении секретных ключей K_e центром доверия. Симметричные шифры разделяют на *поточные,* которые преобразуют каждый символ в потоке исходных данных, и *блочные*, осуществляющие последовательное преобразование блоков данных. В основном применяется блочное шифрование. Оно осуществляется как многократное выполнение типовой процедуры преобразования, называемой раундом шифрования или раундовой функцией шифрования R. Для осуществления блочного шифрования данные представляются в виде последовательности m_i-битовых блоков сообщения $M=\{m_i\}$, $i=\overline{1,n}$. В наиболее широко применяемых шифрах размер выходных блоков равен размеру входных блоков. Минимальной безопасной длиной блока принято считать значение $m_i=64$ бит. Базовыми криптографическими примитивами во многих современных шифрах являются операция подстановки и операция перестановки, которая органически ее дополняет. Блочный шифр, как правило, представляет собой множество подстановок большого размера, заданных на множестве возможных входных блоков, выбираемых от секретного ключа. Временная избыточность, вносимая процессом

симметричного шифрования/расшифрования в информационное окружение сети может быть формализована аддитивной формой

$$t_{\text{убш}} = t_{\text{ш}} + t_{\text{рш}} = n\,R\left(m_i / V_{\text{ш}} + m_i / V_{\text{рш}}\right), \qquad (5)$$

где каждая составляющая моделируется СМОПб вида $t_{\text{ш}} = m_i / V_{\text{ш}}$,с и $t_{\text{рш}} = m_i / V_{\text{рш}}$, с. Здесь m_i-длина i-го блока, бит ($i = \overline{1,n}$, $n = M / m$); $V_{\text{ш}}$, $V_{\text{рш}}$, бит/с – соответственно скорость шифрования/расшифрования; R – число раундов шифрования одного m_i-битового блока. В качестве примеров блочных симметричных шифров на основеуправляемых операций преобразования можно указать шифры ASE, DES, TripleDES, RC2, RC5, RC6, CAST-128, Blowfish, ARCFour,Rijndael, DDP-64, CIKS-1, SPECTR-H64 и другие [32].

Для задания неопределенности хода шифрования информации могут применяться вероятностныешифры [70], в которых в преобразуемое сообщение вводятся случайные данные. Если функция шифрования E_K имеет исходное значение скорости преобразования $V_{\text{ш0}}$, то при использовании шифров с простым вероятностным механизмом скорость шифрования $V^*_{\text{ш}} = V_{\text{ш0}}\left(M^* - r\right)/M^*$, где $M^* = r + M$ – шифруемое сообщение, M –битовый блок открытого сообщения, r-битовый случайный блок. Таким образом, скорость уменьшается в r/M раз, а блоки шифротекста увеличиваются в M^*/M раз (здесь и далее * - будем обозначать защищенный параметр). При вероятностном объединении случайных и информационных битов в зависимости от секретного ключа требует существенного увеличения доли случайных битов (80% и более), что значительно увеличивает время шифрования.

Временная избыточность $t_{\text{убш}}$ должна быть учтена в ограничениях первой и второй задачи анализа на задержку пакетов данных в тракте передачи

$$\theta^{*B}_{st} = \theta^{B}_{st} - t_{\text{убш}} \text{ и } T^{*C}_{st} = T^{C}_{st} - t_{\text{убш}}. \qquad (6)$$

Механизмы контроля целостности данных. Контроль целостности данных – это обнаружение их несанкционированных изменений в процессе передачи. Механизмы «Контроль целостности» вносят как временную, так и протокольную избыточность, связанную с вычислением защитных контрольных сумм (ЗКС) или кодов обнаружения модификаций (КОМ). Существует два типа механизмов обеспечения целостности данных: 1) для защиты целостности отдельного блока данных и 2) для защиты, как целостности отдельного блока данных, так и последовательности потока блоков данных в сеансе связи. Значение криптографических КОМ может

быть получено за один или несколько шагов и является математической функцией криптопеременных и данных.

В МСС формирование/проверка КОМ осуществляется в сеансе связи для каждого пакета данных только в оконечных мультимедийных установках. При этом функции формирования/проверки КОМ, как правило, реализуются в виде соответствующих программ на транспортном или сеансовом уровнях логической структуры сети в оконечных мультимедийных системах (Maltimedia End System, MES). Для обеспечения целостности последовательности блоков данных в протоколах с установлением связи одновременно с КОМ отдельных пакетов используются возможности протоколов с установлением связи: *нумерация*пакетов, *повторная передача*, а также дополнительные средства – *временные или синхронизирующие метки*, обычно используемые для цифровых видео или аудио приложений. Указанный механизм не задействуется при передаче изохронного трафика класса B, ввиду его значительной информационной избыточности. При передаче данных могут быть использованы *отметки времени* в целях обеспечения ограниченной формы защиты против воспроизведения отдельных блоков данных. Этот механизм сам по себе не может защитить от воспроизведения отдельного блока данных. На соответствующих уровнях архитектуры обнаружение манипуляции может привести к задействованию процедуры восстановления как отдельного блока данных, так и последовательности потока блоков данных.

Укажем основные таксоны КОМ – 1) Электронная цифровая подпись (ЭЦП) и ее разновидности (контрольные суммы CRC и коды аутентификации сообщений (message authentication code, MAC), известные также как коды проверки подлинности данных (data authentication code, DAC)); 2) имитозащитные вставки (ИВЗ). Построим модели процессов контроля целостности отдельных блоков данных на примере ИЗВ.

*Имитозащитная вставка*представляет собой k-битовый блок, который вырабатывается по определенному правилу из открытых данных с использованием симметричного секретного ключа, который и гарантирует невозможность (трудность) подделки. Для вычисления имитовставки используется алгоритм, задающий зависимость ИЗВ от каждого бита сообщения. В качестве алгоритма для вычисления имитовставки используется хэш-функция – односторонняя функция $h(M)$, преобразующая сообщение M произвольной длины в выходной хэш-код постоянной длины H с применением или без применения секретных параметров и не позволяющее осуществить обратное преобразование. Могут быть использованы следующие два варианта: 1) *вычисление ИЗВ по открытому тексту* M и 2) *вычисление ИЗВ по шифротексту* M^*. В первом случае отправитель формирует $H_{\text{ИВЗ}i} = h(M)$ за время $t_i^{H\,\text{ИВЗ}1}$. На приеме получатель извлекает M за время$t_j^{M\,\text{ИВЗ}1}$, сам формирует $H_{\text{ИВЗ}i} = h(M)$ за время $t_i^{H\,\text{ИВЗ}1}$ и сравнивает их за время $t_j^{\text{сравн}H\,\text{ИВЗ}2}$. Во втором случае отправитель формирует

$H^*_{\text{ИВЗ2}} = h\left(M^*\right) = h\left(E_{K_i^{\text{ИВЗ2}}}\left(M\right)\right)$, а время его вычисления $t_{\text{ИВЗ1}i}$ включает в себя время $t_i^{M^*\text{ИВЗ2}}$, затрачиваемое на шифрование пакета (сообщения) M, и время $t_i^{H^*\text{ИВЗ2}}$, затрачиваемое на вычисление собственно ИВЗ. Максимальная длина ИЗВ определяется схемой или режимом простой замены и составляет $k = 64$ бит. Значение параметра k (число двоичных разрядов в имитовставки) определяется криптографическими требованиями с учетом того, что вероятность навязывания ложных данных $p = 1/2^k$. На практике, как правило, используют ИЗВ длиной 32 бит (один блок), предоставляющую достаточный ($p = 10^{-9}$) уровень защищенности. На приеме получатель извлекает шифрованное M^* за время $t_j^{M^*\text{ИВЗ2}}$ расшифровывает его на секретном ключе отправителя $K_i^{\text{ИВЗ2}}$ за время $t_j^{M^*\text{ИВЗ2}}$.

Процесс формирования/проверки ИВЗ может быть представлен соответственно двумя аддитивными формами.

$$t^{\text{цел}}_{\text{ИВЗ1}} = t_i^{H\ \text{ИВЗ1}} + t_j^{M\ \text{ИВЗ1}} + t_j^{H\ \text{ИВЗ1}} + t_j^{\text{сравн}H\ \text{ИВЗ2}}, \tag{6}$$

$$t^{\text{цел}}_{\text{ИВЗ2}} = t_i^{M^*\text{ИВЗ2}} + t_i^{H^*\text{ИВЗ2}} + t_j^{M^*\text{ИВЗ2}} + t_j^{M\ \text{ИВЗ2}}. \tag{7}$$

Операция конкатенации КОМ к пакету данных, вносящая протокольную избыточность, может быть формализована аддитивной формой

$$L^{*C} = L^C + S^i. \tag{8}$$

Операция конкатенации КОМ к пакету данных, вносящая протокольную избыточность, может быть формализована аддитивной формой

$$L^{*C} = L^C + S^i. \tag{8}$$

Процессы создания/проверки КОМ моделируются СМОПб и должны быть учтены во второй задаче анализа по аналогии с применением процессов симметричного шифрования.

Моделирование процессов предоставления потоковых механизмов защиты. Построим типовые модели процессов предоставления потоковых механизмов защиты, вносящих потоковую избыточность в информационное окружение сети на примере процесса предоставления *механизмов простой аутентификации без защиты и процессов восстановления целостности*.

Различают услугу аутентификации или подтверждение подлинности равноправных логических объектов (пользователей, приложений), которая реализуется на фазе установления мультимедийного соединения потоковыми механизмами простой и/или строгой аутентификации, и услугу аутентификации отправителя данных в сессии, которая реализуется протокольными механизмами защиты [6,16,27-29]. Протоколы

аутентификации можно классифицировать в соответствии со следующими параметрами [6,16,33,70]: тип аутентификации, тип используемой криптосистемы, вид реализации криптосистемы, количеству обменов служебными сообщениями между субъектами. Дополнительно они могут различаться наличием диалога и доверия между субъектами, а также использованием в протоколах отметок времени. При использовании криптографических процедур они должны сочетаться с протоколами квитирования установления связи, что обеспечивает защиту от воспроизведения. Различают простую и строгую аутентификацию. Простая аутентификация может быть осуществлена без защиты и с защитой.

Простая аутентификация без защиты с центром CA. В случае применения простой аутентификации без защиты с центром *CA* транзакция аутентификации равноправных логических объектов включает в себя следующие фазы: 1) отправитель i передает получателю в открытом (незащищенном) виде свой идентификатор (*имя*)ID_i и (необязательно) *пароль* Pi за время $t_{i,j}^{\text{прд}\,IDi,Pi}$; 2) получатель j передает ID_i и Pi за время $t_{j,CA}^{\text{прд}\,IDi,Pi}$ центру *CA* для сопоставления за время $t_{CA}^{\text{обр}\,Pi}$ с Pi, который хранится у него в качестве атрибута; 3) центр *CA* подтверждает или отрицает получателю j действительность удостоверений за время $t_{CA,j}^{\text{прд}\,Pi}$; 4) успешность или не успешность аутентификации может быть сообщена отправителю i за время $t_{j,i}^{\text{прд}\,Pi}$.

Процесс простой аутентификации с центром *CA* можно формализовать аддитивной формой вида

$$t_{\text{б/з}}^{\text{аут}} = t_{i,j}^{\text{прд}\,IDi,Pi} + t_{j,CA}^{\text{прд}\,IDi,Pi} + t_{CA}^{\text{обр}\,Pi} + t_{CA,j}^{\text{прд}\,Pi} + t_{j,i}^{\text{прд}\,Pi}. \qquad (9)$$

Процессы применения механизмов простой аутентификации без защиты с центром *CA*, порождающие дополнительный трафик безопасности, формализуются в соответствии с их вербальным описанием следующей аддитивной формой

$$\rho_{\text{б/з}}^{\text{аут}} = \rho_{i,j}^{\text{прд}\,IDi,Pi} + \rho_{j,CA}^{\text{прд}\,IDi,Pi} + \rho_{CA,j}^{\text{прд}\,Pi} + \rho_{j,i}^{\text{прд}\,Pi}. \qquad (10)$$

Здесь $\rho_{i,j}^{\text{прд}\,IDi,Pi}$; $\rho_{j,CA}^{\text{прд}\,IDi,Pi}$; $\rho_{CA,j}^{\text{прд}\,Pi}$; $\rho_{j,i}^{\text{прд}\,Pi}$ – соответственно коэффициенты загрузки линейно-цифрового тракта (ЛЦТ) при передаче пароля P_i отправителя i к получателю j; от получателя j к центру CA; от центра CA к получателю j; от получателя j к отправителю i. Каждая фаза передачи трафика безопасности в (9) моделируется СМОУб. Потоковые модели типа (10) должны быть учтены во второй задаче анализа при расчете коэффициента загрузки сети трафиком класса *C* при условии, что приоритеты

обслуживания служебных сообщений безопасности и трафика данных совпадают.

Потоковые модели процессов восстановления целостности передаваемых данных могут быть построены, например, на базе моделей механизмов обратной связи в виде функциональной зависимости $S^{\text{цел}\,k} = f\left(L^{*k}, p_{ij}^{\text{КОМ}}\right)$ [16,69], где L^{*C} – длина защищенного пакета (бит), а $p_{ij}^{\text{КОМ}}$ – вероятность нарушения его целостности, которая в свою очередь зависит от модели нарушителя в сети. Для речевых пакетов будем считать $S^{\text{цел}\,k}=1$, так как для них переспросы не организуются и могут допускаться определенные их потери. Величина $S^{\text{цел}\,k}$ зависит от модели нарушителя и является отдельной научной проблемой, исследование которой выходит за рамки данной работы. Предположим, что вероятность $p_{ij}^{\text{КОМ}} \approx p^{\text{КОМ}}$ для всей МСС одинакова. Если обозначить $p_0^{\text{КОМ}}$ вероятность отсутствия нарушения целостности в кадре длины L^{*C} и предположить, что число переспрашиваемых кадров подчинено геометрическому распределению, то можно показать (для модели тракта передачи с решающей обратной связью)

$$S^{\text{цел}\,C} = -\frac{p_0^{\text{КОМ}}}{1-p_0^{\text{КОМ}}}\ln p_0^{\text{КОМ}}. \qquad (11)$$

Эта потоковая модель процесса восстановления целостности данных должна быть учтена в защищенных моделях логических соединений транспортного уровня МСС при введении механизмов восстановления целостности передаваемых блоков данных класса C в соединении [16,69].

Формализовать процесс восстановления целостности блоков данных класса С можно следующим способом. Пусть пользователь производит повторную попытку передачи пакета приобнаружении нарушения целостности на i-ом транзитном маршрутизаторе с вероятностью $p^{\text{КОМ}}$. Вероятность успешной передачи пакета с n-й попытки равна $\left(p^{\text{КОМ}}\right)^{n-1}\left(1-p^{\text{КОМ}}\right)$, а среднее число повторных попыток на одно соединение для абсолютно настойчивого пользователя

$$M^{\text{КОМ}} = \sum_{n=1}^{\infty} n\left(p^{\text{КОМ}}\right)^{n-1}\left(1-p^{\text{КОМ}}\right). \qquad (12)$$

В этом случае интенсивность $\lambda_{st}^{*C,\text{КОМ}}$ поступления пакетов данных класса С в трактпередачи дается выражением:

$$\lambda_{st}^{*C,\text{КОМ}} = \lambda_{st}^{C}\sum_{n=1}^{\infty} n\left(p^{\text{КОМ}}\right)^{n-1}\left(1-p^{\text{КОМ}}\right) = \frac{\lambda_{st}^{C}}{1-p^{\text{КОМ}}}, \qquad (13)$$

где λ_{st}^{C} – интенсивность поступления пакетов данных класса С в тракт передачи в сессии от отправителя s к получателю t без учета нарушения их целостности.

Таким образом, при необходимости учета процессов восстановления целостности передаваемых сообщений необходимо в моделях логических

соединений уровня межсетевого доступа параметр λ_{st}^{C} в выражении для коэффициентов загрузки тракта передачи ρ_{st}^{C} [16,69] заменить на $\lambda_{st}^{*C,\text{КОМ}}$.

Моделирование процессов предоставления гибридных механизмов защиты. Применение гибридных механизмов защиты вносит как временную и протокольную, так и потоковую избыточность в информационное окружение сети. Построим типовую модель предоставления гибридных механизмов защиты на примере *механизма строгой аутентификации на основе асимметричных ЭЦП с центром СА*.

Строгая аутентификация — опирается на использование криптографической техники для защиты обмена удостоверяющей информации и заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. В соответствии с рекомендациями стандарта X.509 различают процедуры одно-, двух- и трехсторонней строгой аутентификации.

Односторонняя аутентификация предусматривает передачу мандата только в одном направлении. Данный тип аутентификации позволяет подтвердить подлинность отправителя и гарантировать, что мандат (информация, формируемая и передаваемая пользователем в процессе обмена строгой аутентификацией) был фактически сгенерирован отправителем, а также подтвердить подлинность получателя, которому был предназначен мандат отправителя. Дополнительно односторонняя аутентификация позволяет обнаружить нарушение целостности, передаваемой информации и проведение атаки типа «повтор передачи».

Двусторонняя аутентификация устанавливает дополнительно тот факт, что ответный мандат был фактически выработан получателем и предназначен отправителю, а также, что метка времени является «текущей».

Трехсторонняя аутентификация содержит дополнительную передачу дополнительного мандата отправителя и, в отличие от двухсторонней аутентификации, не требует проверки метки времени.

Проведение строгой аутентификации требует обязательного согласования сторонами используемых криптографических алгоритмов и ряда дополнительных параметров. В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

– протоколы на основе симметричных алгоритмов шифрования,
– протоколы на основе однонаправленных ключевых хеш-функций,
– протоколы на основе асимметричных алгоритмов шифрования,
– протоколы на основе алгоритмов электронной цифровой подписи.

Строгая аутентификация на основе асимметричных ЭЦП. ЭЦП S^i – это зашифрованное каким-либо личным (секретным) ключом отправителя Si (не обязательно совпадающего с ключом, использованным для шифрования сообщения) значение хэш-функции $H = h(M)$. Процесс шифрования хэш-кода сообщения и называется подписью S^i. Электронная цифровая подпись

S^i добавляется к мандату M при аутентификации равноправных логических объектов или к пакету L^C при аутентификации отправителя данных и может шифроваться вместе с ним при необходимости сохранения данных в тайне. При этом формируется новое значение мандата $M^* = M + S^i$ и пакета $L^{*C} = L^C + S^i$. Для проверки ЭЦП S^i используется открытый ключ отправителя Pi. Двухключевые криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными пользователями криптосистемы. Использование однонаправленных функций в асимметричных системах ЭЦП не позволяет злоумышленнику вычислить личный ключ отправителя Si, применяемый к хэш-коду. Например, в ЭЦП S^{RSA}. RSA – это задача факторизации, а в ЭЦП S^{EGSA} Эль Гамаля – это задача дискретного логарифмирования. Таким образом, строгая аутентификация здесь основывается на наличии у пользователей аутентифицирующих их личных ключей. Открытые ключи могут быть получены а) по запросу из центра CA или б) переданы непосредственно отправителями в процессе аутентификации Процедура аутентификации в этом случае выглядит следующим образом (временем, затраченным на формированием открытого и секретного ключей пользователем будем пренебрегать).

Рассмотрим обобщенную схему формирования и проверки ассиметричной ЭЦП на примере ЭЦП RSA. Перед отправкой сообщения M вычисляется его хэш-функция $H_i = h(M)$ за время t_i^{Hi}. Затем вычисляется ЭЦП RSA $S^{iRSA} = \mathrm{E}_{\mathrm{Si}}(H_i)$ с применением личного ключа отправителя Si за время t_i^{SiRSA} и мандат ($M_{iRSA}^* = M \square S^{iRSA}$) отправляется получателю за время $t_{i,j}^{\text{прд}MiRSA}$. При получении пары ($M \square S^{iRSA}$) получатель j вычисляет хэш-значение M двумя разными способами. Во-первых, он восстанавливает хэш-код $\tilde{H}_i = \mathrm{D}_{P_i}\left(E_{S_i}(H_i)\right)$, применяя криптографическое преобразование ЭЦП с использованием открытого ключа отравителя P_i за время $t_j^{\tilde{H}i}$. Во-вторых, получатель рассчитывает хэш-значение сообщения $H_j = h(M)$ с помощью аналогичной хэш-функции $h(*)$ за время t_j^{Hj} и сравнивает эти значения за время $t_j^{\text{срравн}H}$. Если эти два значения совпали, получатель считает, что мандат подлинный. Невозможность подделки ЭЦП гарантируется сохранением в тайне личного ключа отправителя S_i, т. е. ответственность возлагается на пользователя.

Любая транзакция аутентификации открытых ключей пользователей в двухключевой криптосистеме, получаемых по запросу из центра сертификации CA включает в себя следующие фазы.

1) Получатель j при получении мандата M_{iRSA}^* запрашивает в CA цифровой сертификат отправителя (содержит открытый ключ P_i и время действия сертификата) за время $t_{j,CA}^{\text{запр}Pi}$.

2) Ответ CA шифруется на личном ключе центра за время $t_{CA}^{\text{обр}Pi}$.

3) Зашифрованное сообщение направляется отправителю за время $t_{CA,j}^{\text{отв}Pi}$.

4) Получатель j, используя открытый ключ центра, который известен каждому, расшифровывает шифрограмму за время $t_j^{\text{аут}CA}$ и получает заверенную версию открытого ключа получателя P_j.

Если центр сертификации CA не участвует, то в этом случае отправитель пересылает свой открытый ключ самостоятельно при передаче мандата M_{iRSA}^*.

Процесс строгой аутентификации с центром CA в этом случае можно формализовать следующей аддитивной формой

$$t_{\text{строг,асимм ЭЦП}}^{\text{аут}CA} = t_i^{Hi} + t_i^{SiRSA} + t_{i,j}^{\text{прд}M*iRSA} + t_{j,CA}^{\text{запр}Pi} + t_{CA}^{\text{обр}Pi} + t_{CA,j}^{\text{отв}Pi} + t_j^{\text{аут}CA} + t_j^{\tilde{H}i} + t_j^{Hj} + t_j^{\text{срвавн}H} \quad (14)$$

Трафик безопасности $\rho_{\text{строг,асим ЭЦП}}^{\text{аут}CA}$ здесь порождается при передаче мандатов и в процессе аутентификации открытых ключей пользователей при обмене с центром CA, а процесс его передачи моделируется трехфазной СМОУб и может быть формализован аддитивной формой вида

$$\rho_{\text{строг,асим ЭЦП}}^{\text{аут}CA} = \rho_{i,j}^{\text{прд}Mi*RSA} + \rho_{j,CA}^{\text{запр}Pi} + \rho_{CA,j}^{\text{отв}Pi}. \quad (15)$$

В этой транзакции процессы вычисления хэш-кода, ЭЦП, их проверки и сравнения моделируются соответствующими СМОПб. Подходы к реализации указанных моделей приведены в [30]. Необходимо отметить, что 1) в зависимости от применяемых процедур одно-, двух- и трехсторонней строгой аутентификации транзакция аутентификации требует обмена от двух до семи служебных сообщений [6]; 2) объем трафика аутентификации, порождаемого при аутентификации равноправных логических объектов, напрямую зависит от величины интенсивности λ_{ij}^{malty} $\left(Mark_{ij}^k = \left\rceil \frac{V_{ij}^{k\min}}{\Theta_{BBU}^{\min}} \right\lceil / \text{час}\right)$ мультимедийных вызовов, которые с учетом потерь создают пропущенную нагрузку (среднее число занятых $\Theta_{BBU}^{\min}$ (бит/с) – базовых минимальных полос пропускания (Basic Bandwisdth Unit, BBU [71,72]) в момент t). Таким образом, каждый мультимедийный вызов резервирует у сети определенную полосу пропускания ЛЦТ для k-ой потоковой компоненты $Mark_{ij}^k = \left\rceil \frac{V_{ij}^{k\min}}{\Theta_{BBU}^{\min}} \right\lceil$ на время средней длительности сеанса t^{ses} (час), т. е. величина полосы пропускания для k-ой потоковой компоненты выражается определенным числом базовых передаточных единиц $\Theta_{BBU}^{\min}$ (бит/с), число которых определяет марка трафика $Mark_{ij}^{malty} = \sum_k \left| \frac{V_{ij}^{k\min}}{\Theta_{BBU}^{\min}} \right| = \left| \frac{V_{ij}^{B\min}}{\Theta_{BBU}^{\min}} \right| + \left| \frac{V_{ij}^{C\min}}{\Theta_{BBU}^{\min}} \right|$. Базовая передаточная единица BBU $\Theta_{BBU}^{\min}$ – это базовая минимальная ширина полосы пропускания, необходимая

для переноса в сети самой «медленной» потоковой компоненты с заданным качеством QoS [73], например, $\Theta_{BBU}^{\min} = 64000$ бит/с.

Поток мультимедийных вызовов λ_{ij}^{malty} порождает в сети пропущенную нагрузку величины $\hat{a}_{ij}^{malty}$ (Эрл) от маршрутизатора i к маршрутизатору j

$$\hat{a}_{ij}^{malty} = N_i \frac{Mark_{ij}^{malty}}{3600} t^{ses} \left(1 - b^{malty}\right) = \left(a^B + a^C\right)\left(1 - b^{multy}\right), \text{ Эрл,} \qquad (16)$$

где $a^B = N_i \frac{Mark_{ij}^{B}}{3600} t^{ses}$ (Эрл), $a^C = N_i \frac{Mark_{ij}^{C}}{3600} t^{ses}$ (Эрл), $V_{ij}^{k\min}$, бит/с – номинальная пропускная способность ЛЦТ, необходимая для обслуживания изохронного трафика класса B ($V_{ij}^{B\min}$, бит/с) и трафика данных класса C ($V_{ij}^{C\min}$,бит/с) (в терминах ATM Forum); b^{malty} – величина допустимых потерь мультимедийного вызова в сети; N_i – количество мультимедийных оконечных устройств (End Maltimedia System, EMS), включенных в машрутизатор i, создающих суммарную нагрузку в направлении маршрутизатора j.

Суммарная величина входящего в сеть потока мультимедийных вызовов задается соответствующей матрицей $Y^{malty} = \left\| a_{ij}^{malty} \right\|$. Предполагается, что в сети применяются методы резервирования канала (Trunk Reservation) с целью введения порогового ограничения доступа $V_{ij}^{k\max}$ к сетевым ресурсам для каждой k-ой потоковой компоненты мультимедийного соединения по критерию суммарного числа базовых передаточных единиц BBU $\Theta_{BBU}^{\min}$ (Sum Limitation Method, SLM) [73-75] с суммарной маркой $Mark_{ij}^{k\max}$.

Каждый мультимедийный вызов порождает поток сообщений аутентификации, создающий соответствующую дополнительную нагрузку в сети $a_{ij}^{\text{аут}}$. Служебные пакеты трафика аутентификации, могут обрабатываться на маршрутизаторах с более низким или равным приоритетом по отношению к пакетам основных потоковых компонент. В предположении, что они обслуживаются в сети с одинаковым приоритетом для пакетов данных класса С, то выражение для нагрузки $a_{ij}^{\text{аут}}$ в общем виде можно представить, как

$$a_{ij}^{\text{аут}} = N_i \frac{Mark_{ij}^{malty}}{3600} T_{ij}^{\text{аут}} M^{\text{аут}}, \text{ Эрл.} \qquad (17)$$

Здесь $T_{ij}^{\text{аут}}$ – непроизводительное время занятия ЛЦТ трафиком безопасности на фазе установления мультимедийного соединения, с (для нашего случая $T_{ij}^{\text{аут}} = T_{ij}^{C}$); $M^{\text{аут}}$ – математическое ожидание числа служебных сообщений трафика безопасности, приходящихся на один мультимедийный вызов, при формализации процессов аутентификации равноправных логических объектов.

Выражение удельной загрузки для трафика аутентификации в этом случае

$$\rho^{\text{аут}} = 1 - \rho_{ij}^{B} - \frac{L^{\text{аут}} + H_{NA}}{T_{ij}^{C} V_{ij}} - \frac{\rho_{ij}^{B}}{1 - \rho_{ij}^{B}} \frac{L^{B} + H_{NA}}{T_{ij}^{C} V_{ij}}.$$

Общая удельная загрузка трафиком данных с учетом трафика аутентификации равна

$$\rho^{*C} = \rho^{C} + \rho_{ij}^{\text{аут}}. \qquad (18)$$

Здесь ρ_{ij}^{B} – удельная загрузка ЛЦТ речевыми пакетами; H_{NA} – заголовок уровневого примитива уровня сетевого доступа, бит; T_{ij}^{C} – заданное среднее время пребывания пакета данных в ЛЦТ, с; V_{ij} – скорость передачи в ЛЦТ, с.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646.

2. Федеральный закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.

3. Федеральный закон РФ «О безопасности» от 28.12.2010 № 39-ФЗ.

4. Федеральный закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

5. Федеральный закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

6. ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. – Введ. 2000-01-01. – М. : ИПК Издательство стандартов, 1999. – 63 с.

7. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введ. 2004-01-01. – М. : ИПК Издательство стандартов, 2002. – 35 с.

8. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 2007-01-01. – М. : Стандартинформ, 2006. – 55 с.

9. ГОСТ Р 51583—2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – Введ. 2014-09-01. – М. : Стандартинформ, 2018. – 14 с.

10. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. – Введ. 1997-07-01. – М. : Издательство стандартов, 1996. – 7 с.

11. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации. М. : Военное изд-во, 1992 (Обновлено: 17 июля 2017г.).

12. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. М. : Военное изд-во, 1992 (Обновлено: 17 июля 2017г.).

13. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. М. : Военное изд-во, 1997 (Обновлено: 17 июля 2017г.).

14. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изм. от 23.03.2017).

15. Мошак, Н. Н. Особенности построения политики информационной безопасности в инфокоммуникационной сети / Н. Н. Мошак, Е. А. Тимофеев // Электросвязь. – 2005. – №9.

16. Мошак, Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез: монография / Н. Н. Мошак. – СПб. : ГУАП, 2014. – 193 с.

17. Мошак, Н.Н. Безопасность информационных систем: учеб. пособие / Н. Н. Мошак. – СПб. : ГУАП, 2019. – 169 с.

18. Зима, В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб. : БХВ-Петербург, 2000. – 320 с.

19. Мошак, Н. Н. Представление сервисов безопасности в пакетных мультисервисных сетях связи в терминах модели взаимодействия открытых систем / Н. Н. Мошак, В. И. Иванов // Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Труды конференции / СПОИСУ. – СПб., 2014. – С. 165-168. ISBN 978-5-906782-28-1.

20. Зайцев, С. С. Сервис открытых информационно-вычислительных сетей: Справочник / С. С. Зайцев, М. И. Кравцунов, С. В. Ротанов. – М.: Радио и связь, 1990. – 240 с.

21. Мошак, Н. Н. Проблемы защиты информационно-телекоммуникационной инфраструктуры РФ от кибератак / Н. Н. Мошак, К. В. Евсейко, А. В. Логинцев // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 3 / СПОИСУ. – СПб., 2017. – 346 с. ISBN 978–5–906931–68–9.

22. Колбанёв, А. М. Проектирование корпоративных информационных систем / А. М. Колбанёв, М. О.Колбанёв, В. В. Цехановский. – СПб. : Изд-во СПбГЭТУ «ЛЭТИ», 2016. – 192 с.

23. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждены требования к защите персональных данных при их обработке в информационных системах персональных данных».

24. Решения IBM для обеспечения информационной безопасности [Электронный ресурс] // URL: www.docplayer.ru/

25. Мошак, Н.Н. Оценка влияния протоколов VPN канального уровня на параметры транспортной системы инфокоммуникационной сети на технологии IP-QoS // Труды учебных заведений связи. – СПб. : СПбГУТ, 2006. – №175.

26. Мошак, Н.Н. Анализ транспортной системы инфокоммуникационной сети на технологии IP-QoS с услугами протоколов VPN / Н. Н. Мошак, Д. Б. Цветков // Деньги и кредит. – 2007. – №8.

27. Мошак, Н.Н. Формализация протоколов простой аутентификации в мультисервисной сети на технологии IP-QoS / Н. Н. Мошак, В. В. Кириллов, Р. С. Кокаева // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Междун.науч.-техн. и научн.-метод.конф., сб. научн. ст. в 4

т. / под ред. С.В. Бачевского. – СПб. : СПбГУТ, 2018. Т2. С. 389-393. ISBN 978-5-89160-169-7.

28. Мошак, Н.Н. Формализация протоколов строгой аутентификации на основе ассиметричных алгоритмов шифрования в мультисервисной сети на технологии IP-QoS / Н. Н. Мошак, В. В. Кириллов, Р. С. Кокаева // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Междун.науч.-техн. и научн.-метод.конф., сб. научн. ст. в 4 т. / под ред. С.В. Бачевского. – СПб. : СПбГУТ, 2018. Т2. С. 393-398. ISBN 978-5-89160-169-7.

29. Мошак, Н. Н. Формализация протоколов строгой аутентификации на основе симметричных алгоритмов шифрования в мультисервисной сети на технологии IP-QoS // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. – СПб., 2018. – С. 94-97. ISBN 978–5–907050–46–4.

30. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. – Введ. 2017-06-01. – М. : Стандартинформ, 2018. – 30 с.

31. Ребриков, К. В. Протоколы автоматического установления контекстов безопасности и управления ключами в Интернете / К. В. Ребриков, В. З. Шнитман // Препринт 19 ИСП РАН. – М., 2007. – 72 с.

32. Фергюстен, Н. Практическая криптография: пер. с англ. Н.Н. Селиной. М. / Н. Фергюстен, Б. Шнайер. – М. : Издательский дом «Вильямс», 2005. – 424 с.

33. Молдовян, А. А. Введение в криптосистемы с открытым ключом / А. А. Молдовян, Н. А. Молдовян. – СПб. : БХВ-Петербург, 2005. – 288 с.

34. Мошак, Н.Н. Формализация и оценка процессов представления механизмов защиты в мультисервисной сети. Общий подход // Электросвязь. – 2012. – №3. – С. 30-35.

35. Защита от несанкционированного доступа к ПК [Электронный ресурс] // URL: www.okbsapr.ru/support/docs/

36. Средство защиты информации SecretNet 6. Руководство администратора. Аудит. / Компания «Код Безопасности», 2010. RU. 88338853.501410.007 91 5.

37. Аппаратно-программный комплекс шифрования Континент Версия 3.5. Руководство администратора. Централизованное управление комплексом / Компания «Код Безопасности», 2010. УВАЛ.00300-104961.

38. Аппаратно-программный комплекс шифрования Континент Версия 3.5. Руководство администратора. Централизованное управление комплексом / Компания «Код Безопасности», 2010. УВАЛ.00300-104963.

39. Антивирус Dr.Web [Электронный ресурс] // URL: products.drweb.com/win/av/

40. Kaspersky Endpoint Security для бизнеса [Электронный ресурс] // URL: http://www.kaspersky.ru/small-to-medium-business-security/endpoint-select/

41. Репин, В. В. Процессный подход к управлению. Моделирование бизнес-процессов / В. В. Репин, В. Г. – М. : РИА «Стандарты и качество», 2008. – 408 с. ISBN 978-5-94938-063-5.

42. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность. – М. : ДМК Пресс, 2004. – 384 с.

43. Глухов, Н. И. Оценка информационных рисков предприятия: учебное пособие / Н. И. Глухов. – Иркутск: ИрГУПС, 2013. – 148 с.

44. Единая система мониторинга информационной безопасности территориального учреждения Банка России. Общее описание системы / ООО «НПФ «Кристалл». МПИФ.42 5790.064.ПД.2.

45. Мошак, Н. Н.Организация мониторинга информационной безопасности в Главном управлении Банка России по Ленинградской области / Н. Н. Мошак, А. В. Перервенко // Информационно-аналитический бюллетень Вестник Северо-Запада. – 2013. – №4 (63). – С. 19-27.

46. Мошак, Н.Н. Системы мониторинга информационной безопасности в территориальных учреждениях Банка России // Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2014. – С. 189-190. ISBN 978-5-906555-02-1.

47. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационные технологии. Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий. – Введ. 01.09.2007. – М. : Стандартинформ, 2007. – 76 с.

48. ISO/IEC 27001. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – Введ. 06.01.2005. – М. : Стандартинформ, 2006. – 54 с.

49. Кононов, А. А. Страхование нового века. Как повысить безопасность информационной инфраструктуры // Connect. – 2001. – №12.

50. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2-2009 (приняты и введены в действие Распоряжением Банка России от 11.11.2009 N Р-1190).

51. BS 7799-2:2005. Спецификация системы управления информационной безопасностью. – Введ. 01.07.2005. – Англия. – 2005. – 86 с.

52. OCTAVE(Система Операционной Оценки Критических Угроз, Активов и Уязвимостей) / SoftwareEngineeringInstitute, CarnegieMellonUniversity.

53. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology: NIST 800-30. – Введ. 06.01.2002. – США. – 2002. – 56 с.

54. CRAMM (Risk Analysis and Management Method) / UK Government.

55. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ. [Электронныйресурс]. URL: http://www.ixbt.com/cm/ informationsystem-risks012004.shtml/

56. netForensics [Электронный ресурс] // URL: www.netforensics.com/

57. Networkintelligence [Электронный ресурс] // URL: http://www.network-intelligence.com

58. Интеллектуальные Системы Безопасности ISS [Электронный ресурс] // URL: http://www.iss.net

59. SASVisualAnalytics [Электронный ресурс] // URL: http://www.visualanalytics.com

60. Птицына, Л. К. Обеспечение информационной безопасности на основе методологического базиса агентных технологий / Л. К. Птицына, А. В. Птицын // Вестник Брянского государственного технического университета. – 2017. – № 2 (55). – С. 146-154.

61. Птицына, Л. К. Распределённый модельно-аналитический интеллект комплексных систем защиты информации / Л. К. Птицына, Д. С. Гусев // Юбилейная X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России-2017».: Материалы конференции / СПОИСУ. – СПб. : Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), 2017. – С. 528-530.

62. Ptitsyna L., Lebedeva A., Belov M., Ptitsyn A. Information agent reaction research under the influence of information and communication environment // II International Conference on Control in Technical Systems (CTS). – 2017. – PP. 20-23.

63. Александров, А. М. Безопасность сетей связи и некоторые задачи теории телетрафика // Электросвязь. – 2003. – №12. – С. 20-21.

64. Птицын, А. В. Аналитическое моделирование комплексных систем защиты информации. – Монография / А. В. Птицын, Л. К. Птицына. – Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. – 293 с.

65. Птицына, Л. К. Определение временного профиля критических ситуаций в мультиагентной системе защиты информации / Л. К. Птицына, Д. С. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. / Под ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич. – СПб. : СПбГУТ, 2018. – Т. 2. – С. 288-292.

66. Птицына, Л. К.Объектно-ориентированный анализ интеграции средств защиты информации / Л. К. Птицына, А. В. Птицын // Вопросы защиты информации. – М.: Изд-во ВИМИ, 2013. – № 1. – С. 79-86.

67. Мошак, Н. Н. Методология моделирования и анализа процессов функционирования пакетных мультисервисных сетей / Н. Н. Мошак, А. И. Яшин, Е. В. Давыдова // Электросвязь. – 2015. – №4. – С. 35-39.

68. Мошак, Н. Н. Методы и алгоритмы анализа и синтеза пакетных мультисервиных сетей NGN / Н. Н. Мошак, А. И. Яшин, Е. В. Давыдова // Электросвязь. – 2015. – №11. – С. 46-52.

69.Мошак, Н.Н. Модели, методы и алгоритмы анализа процессов функционирования инфотелекоммуникационных транспортных систем: дис. 05.13.13 докт. тех. наук: защищена 16.12.2009. утв. 09.04.2010 / Мошак Николай Николаевич. Л., 2009. – 345 с.

70.Молдавян, А. А. Криптография: от примитивов к синтезу алгоритмов / А. А. Молдовян, Н. А. Молдовян, М. А. Еремеев. – СПб. : БХВ-Петербург, 2004. – 448 с.

71. Мейкшан, В. И. Оценка показателей качества функционирования мультисервисных сетей связи при фиксированной маршрутизации / В. И. Мейкшан, В. В. Столяров // Инфокоммуникационные технологии. – 2006. – Том 4. – №4. – С. 44-48.

72. Мейкшан, В. И. Оценка влияния повторных вызовов на функционированиемультисервисной сетис адаптивной маршрутизацией / В. И. Мейкшан, П. А. Ищук, С. В. Шедоева. // Вестник СибГУТИ. – 2012. – №2. – С. 5-61.

73. Ершов, В. А. Метод расчета пропускной способности звена Ш-ЦСИС с технологией АТМ при мультисервисном обслуживании / В. А. Ершов, Э. Б. Ершова, В. В. Ковалев // Электросвязь. – 2000. – №3. – С.29-23.

74. Ершов, В.А. Управление канальными ресурсами ЦСИС на основе его резервирования / В. А. Ершов, Д. В. Ершов // Электросвязь – 1994. – №12. – С. 1-8.

75. Ершов, В.А. Теоретические основы построения цифровой сети с интеграцией служб (ISDN) / В. А. Ершов, Н. А. Кузнецов. – М.: Институт проблем передачи информации РАН. – 1995. – 280 с.

Оглавление

Мошак Николай Николаевич
Птицына Лариса Константиновна

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Учебное пособие

Ответственный редактор д. т. н., проф. А. А. Гоголь

Редактор *И. И. Щенсняк*

План издания 2020 г., доп. п. 3
Подписано к печати ……
Объем ….. усл.-печ. л. Тираж 28 экз. Заказ ….
Редакционно-издательский отдел СПбГУТ
193232 СПб., пр. Большевиков, 22
Отпечатано в СПбГУТ