Концепция обеспечения информационной безопасности колледжа

Настоящий документ представляет собой концепцию обеспечения информационной безопасности предприятия и определяет:

Основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для предприятия.

Основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (ИБ) и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности (СОИБ) предприятия.

Модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования.

Модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба.

Требования безопасности, определяемые по результатам анализа рисков.

Меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований.

Ответственность сотрудников предприятия за соблюдение установленных требований ИБ при эксплуатации информационной системы (ИС) предприятия.

Общие положения

СОИБ предприятия представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов предприятия от угроз информационной безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных документированной политикой информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Экономический эффект от внедрения СОИБ должен проявляться в виде снижения величины возможного материального, репутационного и иных видов ущерба, наносимого предприятию, за счет использования мер, направленных на формирование и поддержание режима ИБ. Эти меры призваны обеспечить:

доступность информации (возможность за приемлемое время получить требуемую информационную услугу);

целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

конфиденциальность информации (защита от несанкционированного ознакомления);

неотказуемость (невозможность отрицания совершенных действий);

аутентичность (подтверждение подлинности и достоверности электронных документов).

Концепция ИБ предприятия определяет состав критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты информации (СЗИ) и системы организационных мероприятий является предметом конкретных проектов и политик информационной безопасности, разрабатываемых на основе данной Концепции.

Настоящая концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития информационных систем (ИС) предприятия. Рекомендуемый срок пересмотра концепции составляет три года (при условии отсутствия коренных изменений в структуре системы, в технологиях управления и передачи информации).

Подготовка настоящего документа, внесение в него изменений и общий контроль выполнения требований по обеспечению ИБ предприятия осуществляется сотрудниками отдела ИБ предприятия.

Ответственность за выполнение требований ИБ, определяемых настоящей Концепцией и другими организационно-распорядительными документами предприятия, возлагается на пользователей и администраторов корпоративной сети передачи данных предприятия, а также их руководителей.

Перечень необходимых мер защиты информации определяется по результатам аудита информационной безопасности ИС предприятия и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения доступности информации и работоспособности программно-технических средств, обрабатывающих эту информацию.

Стратегия обеспечения ИБ должна строиться в соответствии с Российским законодательством в области защиты информации, требованиями международных, отраслевых и технологических стандартов.

Настоящая концепция разработана на основе нормативных и распорядительных документов в области информационной безопасности Российской Федерации.

Описание объекта защиты

Объектом защиты являются автоматизированные системы (как собственной, так и сторонней разработки), входящие в состав информационной системы предприятия.

Информационная система предприятия представляет собой совокупность территориально разнесенных объектов, информационный обмен между которыми осуществляется посредством использования открытых каналов связи, предоставленных сторонними операторами электросвязи. Передача информации осуществляется в кодированном виде на основе протокола кодирования, проверки целостности и конфиденциальности информационных потоков HASH64. Кодирование входящих и исходящих информационных потоков осуществляется на магистральных маршрутизаторах.

Назначение и основные функции информационной системы

ИС предназначена для обеспечения работоспособности информационной инфраструктуры предприятия, предоставления сотрудникам структурных подразделений различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов предприятия.

Группы задач, решаемых в информационной системе

Корпоративная сеть предприятия предназначена для обеспечения автоматизации бизнес процессов организационной структуры предприятия. Решение функциональных задач реализуется на базе информационной инфраструктуры корпоративной сети с использованием специализированных программных приложений и общедоступных информационных сервисов.

К специализированным приложениям относится система бухгалтерского учета, геоинформационная система, а также система электронного документооборота на базе сервисного программного обеспечения Lotus Notes Server.

К общедоступным сетевым сервисам относятся средства обработки информационных потоков на сетевом и операционном уровне, такие как:

Система обмена электронной почтой на основе специализированных протоколов Lotus внутри предприятия и протокола SMTP для внешнего информационного обмена.

Файловый сервис на основе протоколов Netware.

Классификация пользователей системы

Пользователем ИС является любой сотрудник предприятия, зарегистрированный в сети, в соответствии с установленным порядком, и прошедший идентификацию в службе каталогов, которому предоставляется доступ к информационным ресурсам корпоративной сети и приложениям, в соответствии с его должностными обязанностями.

Доступ к специализированным автоматизированным системам утверждается руководством департамента ИТ в соответствии должностными инструкциями, утвержденными руководством предприятия.

Особую категорию пользователей корпоративной сети составляет руководство предприятия. АРМ данной категории пользователей подключены к ИС и нуждаются в использовании дополнительных (усиленных) мер защиты информации, с целью предотвращения кражи информации, составляющей коммерческую тайну предприятия.

Организационная структура обслуживающего персонала

Административно-техническая поддержка ИС предприятия осуществляется департаментом информационных технологий, в состав которого входят:

Отдел развития и эксплуатации информационных систем.

Отдел информационной безопасности.

Отдел технической поддержки.

Информационно-аналитический отдел.

Сотрудники отделов информационных технологий филиалов предприятия.

Структура и состав комплекса программно-технических средств

ИС объекта защиты включает в себя корпоративную сеть предприятия в составе:

Серверы.

Рабочие станции.

Линии связи и активное сетевое оборудование.

Магистральные средства передачи данных.

Корпоративную телефонную систему.

Корпоративная сеть предприятия

В качестве базового сетевого протокола в корпоративной сети используется протокол TCP/IP.

В качестве адресного пространства используется сеть класса A – 10.0.0.0/8, определенная документом IETF RFC 1597 для частных IP-сетей. В корпоративной сети предприятия выделяются следующие типы адресных пространств:

адресные пространства, выделенные филиальным фрагментам;

адресные пространства, выделенные аппарату управления предприятием;

адресное пространство для адресации магистрального сегмента корпоративной сети;

резервное адресное пространство.

Используемая схема распределения адресного пространства маркируется следующим образом 10.x.y.z, где: x – номер филиала; y – номер виртуальной сети (VLAN) внутри филиала; z – номер устройства внутри виртуальной сети.

Серверы

Серверная группа корпоративной сети работает под управлением ОС Microsoft Windows. Функционально она подразделяется на серверы поддержки специализированных приложений, серверы поддержки общедоступных сервисов и серверы, поддерживающие технологические службы корпоративной сети.

Рабочие станции

К информационной системе предприятия подключены автоматизированные рабочие места пользователей, функционирующих на базе ОС Microsoft Windows XP.

Линии связи и активное сетевое оборудование

Основу ИС составляет стек коммутаторов Cisco Catalyst, производства компании Cisco Systems Inc.

Выделенные магистральные каналы обмена данными используются для обеспечения внешнего информационного взаимодействия ИС с филиалами предприятия, районными эксплуатационными службами, а также для доступа к глобальной информационной сети Интернет.

Виды информационных ресурсов, хранимых и обрабатываемых в системе

В ИС предприятия хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации.

К конфиденциальной и служебной информации, циркулирующей в КСПД, 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 строго конфиденциальной 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, проводимой ей политики и, в конечном счете, привести к ее краху.

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

Структура информационных потоков

Внутренние информационные потоки

Внутри ИС выделяются следующие информационные потоки:

Передача файлов между файловыми серверами и пользовательскими рабочими станциями по протоколу SMB (протокол открытого обмена информацией между АРМ пользователей и серверами на основе стека TCP/IP).

Передача сообщений электронной почты, посредством использования хешированного соединения программного обеспечения Lotus Notes.

Передача юридической и справочной информации между серверами БД и пользовательскими рабочими станциями.

Деловая переписка.

Передача отчетной информации.

Передача бухгалтерской информации между пользовательскими рабочими станциями и сервером БД в рамках автоматизированных систем «1С Бухгалтерия», «1С Зарплата и Кадры», «Оперативный учет».

Внешние информационные потоки

В качестве внешних информационных потоков используются:

Передача отчетных документов (производственные данные) от филиалов предприятия, по каналам корпоративной сети, а также с использованием магнитных носителей.

Передача платежных документов в Банки.

Передача финансовых и статистических отчетных документов от филиалов предприятия;

Внутриведомственный и межведомственный обмен электронной почтой.

Передача информации по коммутируемым каналам удаленным пользователям.

Различные виды информационных обменов между ИС и сетью Интернет.

Характеристика каналов взаимодействия с другими системами и точек входа

В ИС предприятия используются следующие каналы взаимодействия с внешними сетями:

Выделенный магистральный канал взаимодействия с корпоративной сетью, посредством использования технологии VPN.

Резервная линия связи с сетью Интернет.

Коммутируемый канал связи, посредством использования технологии GPRS.

Защита подключений к внешним сетям осуществляется при помощи МЭ и встроенных средств защиты магистрального роутера.

Доступ к информационным ресурсам сети Интернет открыт для всех пользователей ИС, посредством использования кеширующего прокси сервера на основе программного обеспечения Squid.

Основные факторы, влияющие на информационную безопасность предприятия

Основными факторами, влияющими на информационную безопасность предприятия, являются:

расширение сотрудничества предприятия с партнерами;

автоматизация бизнес-процессов на предприятии;

расширение кооперации исполнителей при построении и развитии информационной инфраструктуры предприятия;

рост объемов информации предприятия, передаваемой по открытым каналам связи;

рост компьютерных преступлений.

Основные принципы обеспечения информационной безопасности

Построение архитектуры СОИБ предприятия должно базироваться на соблюдении следующих основных принципов обеспечения ИБ:

Простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов сетевого взаимодействия. Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного развития).

Апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

Построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью.

Управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей.

Простота эксплуатации, автоматизация максимального числа действий администраторов сети.

Эшелонированность обороны – для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств – системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода систем в незащищенное состояние.

Равнопрочность обороны по всем направлениям – осуществляется регламентация и документирование всех способов доступа к ресурсам корпоративной сети. В соответствии с этим принципом запрещается создавать несанкционированные подключения к корпоративной сети и другими способами нарушать установленный порядок предоставления доступа к информационным ресурсам, который определяется «Политикой управления доступом к ресурсам корпоративной сети», «Политикой обеспечения ИБ при взаимодействии с сетью Интернет» и «Политикой обеспечения ИБ удаленного доступа к ресурсам корпоративной сети предприятия».

Профилактика нарушений безопасности – в большинстве случаев для предприятия экономически оправданным является принятие предупредительных мер по недопущению

нарушений безопасности в отличие от мер по реагированию на инциденты, связанных с принятием рисков осуществления угроз информационной безопасности. Однако это не исключает необходимости принятия мер по реагированию на инциденты и восстановлению поврежденных информационных ресурсов. В соответствии с данным принципом должен проводиться анализ рисков, опирающийся на модель угроз безопасности и модель нарушителя, определяемые настоящей Концепцией. Многие риски можно уменьшить путем принятия превентивных мер защиты.

Минимизация привилегий - политика безопасности должна строиться на основе принципа «все, что не разрешено, запрещено». Права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей;

Разделение обязанностей между администраторами корпоративной сети, определяется должностными инструкциями и регламентами администрирования.

Экономическая целесообразность. Обеспечение соответствия ценности информационных ресурсов предприятия и величины возможного ущерба (от их разглашения, утраты, утечки, уничтожения и искажения) уровню затрат на обеспечение информационной безопасности. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы автоматизированных систем предприятия, в которых эта информация циркулирует.

Преемственность и непрерывность совершенствования. Обеспечение постоянного совершенствования мер и средств защиты информационных ресурсов и информационной инфраструктуры на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования систем защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого передового отечественного и зарубежного опыта в этой области. При выборе программно-технических решений по обеспечению ИБ предприятия, предпочтение отдается решениям, обеспечивающим соблюдение основных принципов ИБ, а также удовлетворяющих следующим критериям:

Поддержка международных, национальных, промышленных и Интернет стандартов (предпочтение отдается международным стандартам).

Поддержка наибольшей степени интеграции с корпоративными программно-аппаратными платформами и используемыми СЗИ;

Унификация разработчиков и поставщиков используемых продуктов.

Унификация средств и интерфейсов управления подсистемами ИБ.

Организация работ по защите информации

Организация и проведение работ по обеспечению ИБ предприятия определяются настоящей концепцией, действующими государственными и международными стандартами и другими нормативными и методическими документами.

Организация работ по обеспечению ИБ возлагается на руководителя департамента информационных технологий, осуществляющего эксплуатацию и сопровождение ИС, а

методическое руководство и контроль над эффективностью предусмотренных мер защиты информации - на руководителя отдела ИБ предприятия.

Эксплуатация ИС предприятия осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в соответствующих разделах настоящего документа.

Комплекс мер по защите информации на предприятии включает в себя следующие мероприятия:

Назначение ролей и распределение ответственности за использование информационных ресурсов корпоративной сети.

Разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и других документов по обеспечению ИБ.

Подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ.

Проектирование, развертывание и совершенствование технической инфраструктуры СОИБ.

Аудит состояния ИБ предприятия.

Техническая инфраструктура СОИБ предназначена для решения следующих задач:

Защиты внешнего периметра корпоративной сети предприятия от угроз со стороны внешних сетей за счет использования межсетевого экранирования, контроля удаленного доступа и мониторинга информационных взаимодействий.

Защиты корпоративных серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам корпоративных серверов, механизмов мониторинга и аудита безопасности.

Комплексной антивирусной защиты систем, входящих в состав корпоративной сети за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по следующим уровням:

Защиты внешнего шлюза в сеть Интернет.

Защиты корпоративных серверов.

Защиты рабочих мест пользователей.

Мониторинга сетевого трафика в реальном масштабе времени с целью выявления злоумышленных действий пользователей корпоративной сети и попыток осуществления НСД к ресурсам корпоративной сети со стороны внешних злоумышленников.

Защиты прикладных подсистем, функционирующих в составе корпоративной сети, обеспечение доступности предоставляемых ими прикладных сервисов.

Защиты межсетевых взаимодействий между сегментами ИС предприятия.

Меры обеспечения информационной безопасности

Меры обеспечения информационной безопасности организационного уровня

СОИБ реализуется путем сочетания мер организационного и программно-технического уровней. Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня, то есть мер, предпринимаемых руководством предприятия, является политика информационной безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию предприятия в области ИБ, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности предприятия определяется настоящим документом, а также другими нормативными и организационно-распорядительными документами предприятия, разрабатываемыми на основе настоящей концепции. К числу таких документов относятся следующие:

Политика защиты от НСД к информации;

Политика предоставления доступа пользователей в ИС;

Политика управления паролями;

Политика восстановления работоспособности АС в случае аварии;

Политика резервного копирования и восстановления данных;

Политика предоставления доступа к ресурсам сети Интернет;

Политика управления доступом к информационным ресурсам ИС предприятия;

Политика внесений изменений в программное обеспечение;

Политика управления доступом к АРМ Пользователя;

Политика использования электронной почты;

Политика анализа защищенности ИС предприятия;

Программа, методика и регламенты тестирования функций СЗИ от НСД к информации;

Инструкция, определяющая порядок и правила регистрации распечатываемых документов, содержащих конфиденциальную информацию, в соответствии с перечнем информации, составляющей конфиденциальную и служебную информацию;

Должностные инструкции для операторов, администраторов и инженеров, осуществляющих эксплуатацию и обслуживание ИС предприятия;

Инструкции для операторов, администраторов и инженеров по обеспечению режима информационной безопасности;

Документированная процедура контроля целостности программной и информационной частей ИС предприятия.

Меры обеспечения информационной безопасности процедурного уровня

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

управление персоналом;

физическая защита;

поддержание работоспособности;

реагирование на нарушения режима безопасности;

планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого сотрудника предприятия необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.

Информационная безопасность ИС предприятия зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.

При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты офисных зданий и других помещений, принадлежащих предприятию, по следующим направлениям:

физическое управление доступом;

противопожарные меры;

защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

поддержка пользователей ИС;

поддержка программного обеспечения;

конфигурационное управление;

резервное копирование;

управление носителями;

документирование;

регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима информационной безопасности преследует две главные цели:

блокирование нарушителя и уменьшение наносимого вреда;

недопущение повторных нарушений.

На предприятии должен быть выделен сотрудник, доступный 24 часа в сутки, отвечающий за реакцию на нарушения. Все пользователи ИС должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В случае невозможности связи с данным сотрудником, должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.

Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.

Механизмы контроля, существенные для предприятия с юридической точки зрения, включают в себя:

Защиту данных и тайну персональной информации;

Охрану документов организации;

Права на интеллектуальную собственность.

В соответствии с международным стандартом ISO 17799, а также руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

Политика информационной безопасности;

Распределение ролей и ответственности за обеспечение информационной безопасности;

Обучение и тренинги по информационной безопасности;

Информирование об инцидентах безопасности;

Управление непрерывностью бизнеса.

Меры обеспечения информационной безопасности программно-технического уровня
Программно-технические средства защиты располагаются на следующих рубежах:

Защита внешнего периметра КСПД;

Защита внутренних сетевых сервисов и информационных обменов;

Защита серверов и рабочих станций;

Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;

Защита выделенного сегмента руководства компании.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

идентификация/аутентификация пользователей ИС;

разграничение доступа объектов и субъектов информационного обмена;

протоколирование/аудит действий легальных пользователей;

экранирование информационных потоков и ресурсов КСПД;

туннелирование информационных потоков;

шифрование информационных потоков, критической информации;

контроль целостности;

контроль защищенности;

управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему предприятия от внешнего мира.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже, если по каким-либо причинам, она окажется успешной. Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС предприятия должна

предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).

Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

Распределение ответственности и порядок взаимодействия

Ответственным за разработку мер и контроль над обеспечением защиты информации является руководитель УИТ. Специалистами УИТ осуществляются следующие виды работ по защите информации:

Контроль защищенности ИТ инфраструктуры предприятия от угроз ИБ осуществляется посредством:

Проведения аудита безопасности ИС;

Контроля выполнения правил утвержденных политик безопасности администраторами и пользователями корпоративной сети;

Контроля доступа к сетевым ресурсам.

Предотвращение, выявление, реагирование и расследование нарушений ИБ посредством:

Анализа и мониторинга журналов аудита критичных компонентов корпоративной сети, включая активное сетевое оборудование, МЭ, серверы, рабочие станции и т.п.;

Мониторинга сетевого трафика с целью выявления сетевых атак;

Контроля процесса создания новых учетных записей пользователей и предоставления доступа к ресурсам корпоративной сети;

Опроса пользователей и администраторов информационных систем;

Внедрения и эксплуатации специализированных программных и программно-технических средств защиты информации;

Координации деятельности всех структурных подразделений предприятия по поддержанию режима ИБ.

Менеджером информационной безопасности осуществляется планирование и реализация организационных мер по обеспечению ИБ, включая:

Анализ и управление информационными рисками;

Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов и других организационно-распорядительных документов по обеспечению ИБ;

Разработку планов мероприятий по повышению уровня ИБ предприятия;

Обучение пользователей информационных систем, с целью повышения их осведомленности в вопросах ИБ.

Наряду с УИТ, в разработке и согласовании организационно-распорядительных и нормативных документов по защите информации, включая составление перечней информационных ресурсов подлежащих защите, также участвуют следующие подразделения предприятия:

Служба безопасности;

Юридическое управление;

Отдел кадров;

Функциональные подразделения, в которых обрабатывается информация, требующая защиты.

Квалификационные требования, предъявляемые к сотрудникам подразделений, отвечающих за обеспечение ИБ, содержатся в должностных инструкциях. Специалисты по защите информации должны проходить регулярную переподготовку и обучение.

Предоставление, изменение, отмена и контроль доступа к ресурсам корпоративной сети передачи данных производится сотрудниками УИТ исключительно по утвержденным заявкам, в соответствии с «Политикой предоставления доступа пользователей в КСПД».

Сотрудники УИТ отвечают за осуществление настройки параметров информационной безопасности серверов и рабочих станций корпоративной сети передачи данных, в соответствии с утвержденными корпоративными стандартами, определяющими требуемые уровни обеспечения защиты информации для различных структурных и функциональных компонентов корпоративной сети. ОТиИБ УИТ отвечает за разработку соответствующих спецификаций и рекомендаций по настройке параметров безопасности, а также за осуществление контроля их исполнения.

Обеспечение внешних подключений корпоративной сети передачи данных предприятия к сети Интернет и другим внешним сетям, предоставление сотрудникам удаленного доступа к корпоративной сети и организация VPN-каналов связи осуществляется сотрудниками УИТ с соблюдением требований информационной безопасности, определяемых

«Политикой предоставления доступа к ресурсам сети Интернет» и «Политикой управления доступом к информационным ресурсам КСПД».

Договоры на обслуживание клиентов заключаются по утвержденной типовой форме функциональными подразделениями. Если договоры предполагают электронное обслуживание с использованием технологических ресурсов предприятия, то организация и контроль процедур безопасности осуществляется сотрудниками ОТиИБ УИТ.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к конфиденциальной информации, либо к ИС предприятия, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима ИБ при выполнении работ в ИС». Подготовка типовых вариантов этих соглашений осуществляется УИТ предприятия, совместно с юридическим управлением.

Порядок категорирования защищаемой информации

Различаются следующие категории информационных ресурсов, подлежащих защите в предприятия:

Информация, составляющая коммерческую тайну;

Информация, составляющая служебную тайну;

Персональные данные сотрудников;

Конфиденциальная информация (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне;

Данные, критичные для функционирования ИС и работы бизнес подразделений.

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

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

В первую очередь к коммерческой информации относятся:

Знания и опыт в области реализации продукции и услуг;

Сведения о конъюнктуре рынка, маркетинговые исследования;

Анализ конкурентоспособности продукции и услуг;

Информация о потребителях, заказчиках и посредниках;

Банковские отношения, кредиты, ссуды, долги;

Знание наиболее выгодных форм использования денежных средств, ценных бумаг, акций, капиталовложений;

Бухгалтерские и финансовые отчеты, сведения о зарплате;

Предполагаемые объемы коммерческой деятельности, материалы договоров (условия, реализация, порядок передачи продукции);

Списки клиентов и деловая переписка;

Цены и расценки, формы и виды расчетов.

Правила отнесения информации к коммерческой тайне и порядок работы с документами, составляющими коммерческую тайну, определяются «Инструкцией по обеспечению режима конфиденциальности», «Положением о конфиденциальности», а также «Перечнем конфиденциальных сведений».

Подходы к решению проблемы защиты информации на предприятии, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования бизнес процессов предприятия. Для этого выполняются следующие мероприятия:

Определяется порядок работы с документами, образцами, изделиями и др., содержащими конфиденциальные сведения;

Разрабатываются правила категорирования информации, позволяющие относить ее к различным видам конфиденциальных сведений и определять степень ее критичности для предприятия;

Устанавливается круг лиц и порядок доступа к подобной информации;

Вырабатываются меры по контролю обращения документов, содержащих конфиденциальные сведения;

В трудовые договоры с сотрудниками включаются обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации содержится в трудовом договоре, который подписывается всеми сотрудниками при приеме на работу.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Компанией с другими организациями.

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

На предприятии должен быть документально оформлен «Перечень конфиденциальных сведений». Все работники должны быть ознакомлены с этим перечнем в части их касающейся.

Ответственность за составление «Перечня конфиденциальных сведений» несет руководитель УИТ.

Модель нарушителя информационной безопасности

Под нарушителем ИБ понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам предприятия.

Под атакой на ресурсы корпоративной сети понимается попытка нанесения ущерба информационным ресурсам систем, подключенных к сети. Атака может осуществляться как непосредственно нарушителем, так и опосредованно, при помощи процессов, выполняющихся от лица нарушителя, либо путем внедрения в систему программных или аппаратных закладок, компьютерных вирусов, троянских программ и т. п.

В соответствии с моделью, все нарушители по признаку принадлежности к подразделениям, обеспечивающим функционирование ИС, делятся на внешних и внутренних.

Внутренние нарушители

Внутренним нарушителем может быть лицо из следующих категорий сотрудников обслуживающих подразделений:

обслуживающий персонал (системные администраторы, администраторы БД, администраторы приложений и т.п., отвечающие за эксплуатацию и сопровождение технических и программных средств);

программисты, отвечающие за разработку и сопровождение системного и прикладного ПО;

технический персонал (рабочие подсобных помещений, уборщицы и т. п.);

сотрудники бизнес подразделений предприятия, которым предоставлен доступ в помещения, где расположено компьютерное или телекоммуникационное оборудование.

Предполагается, что несанкционированный доступ на объекты системы посторонних лиц исключается мерами физической защиты (охрана территории, организация пропускного режима и т. п.).

Предположения о квалификации внутреннего нарушителя формулируются следующим образом:

внутренний нарушитель является высококвалифицированным специалистом в области разработки и эксплуатации ПО и технических средств;

знает специфику задач, решаемых обслуживающими подразделениями ИС предприятия;

является системным программистом, способным модифицировать работу операционных систем;

правильно представляет функциональные особенности работы системы и процессы, связанные с хранением, обработкой и передачей критичной информации;

может использовать как штатное оборудование и ПО, имеющиеся в составе системы, так и специализированные средства, предназначенные для анализа и взлома компьютерных систем.

В зависимости от способа осуществления доступа к ресурсам системы и предоставляемых им полномочий внутренние нарушители подразделяются на пять категорий.

Категория А: не зарегистрированные в системе лица, имеющие санкционированный доступ в помещения с оборудованием. Лица, относящиеся к категории А могут: иметь доступ к любым фрагментам информации, распространяющейся по внутренним каналам связи корпоративной сети; располагать любыми фрагментами информации о топологии сети, об используемых коммуникационных протоколах и сетевых сервисах; располагать именами зарегистрированных пользователей системы и вести разведку паролей зарегистрированных пользователей.

Категория В: зарегистрированный пользователь системы, осуществляющий доступ к системе с удаленного рабочего места. Лица, относящиеся к категории В: располагают всеми возможностями лиц, относящихся к категории А; знают, по крайней мере, одно легальное имя доступа; обладают всеми необходимыми атрибутами, обеспечивающими доступ к системе (например, паролем); имеют санкционированный доступ к информации, хранящейся в БД и на файловых серверах корпоративной сети, а также на рабочих местах пользователей. Полномочия пользователей категории В по доступу к информационным ресурсам корпоративной сети предприятия должны регламентироваться политикой безопасности, принятой на предприятии.

Категория C: зарегистрированный пользователь, осуществляющий локальный либо удаленный доступ к системам входящим в состав корпоративной сети. Лица, относящиеся к категории C: обладают всеми возможностями лиц категории B; располагают информацией о топологии сети, структуре БД и файловых систем серверов; имеют возможность осуществления прямого физического доступа к техническим средствам ИС.

Категория D: зарегистрированный пользователь системы с полномочиями системного (сетевого) администратора. Лица, относящиеся к категории D: обладают всеми возможностями лиц категории C; обладают полной информацией о системном и прикладном программном обеспечении ИС; обладают полной информацией о технических средствах и конфигурации сети; имеют доступ ко всем техническим и программным средствам ИС и обладают правами настройки технических средств и ПО. Концепция безопасности требует подотчетности лиц, относящихся к категории D и осуществления независимого контроля над их деятельностью.

Категория E: программисты, отвечающие за разработку и сопровождение общесистемного и прикладного ПО, используемого в ИС. Лица, относящиеся к категории E: обладают возможностями внесения ошибок, программных закладок, установки троянских программ и вирусов на серверах корпоративной сети; могут располагать любыми фрагментами информации о топологии сети и технических средствах ИС.

Внешние нарушители

К внешним нарушителям относятся лица, пребывание которых в помещениях с оборудованием без контроля со стороны сотрудников предприятия невозможно.

Внешний нарушитель: осуществляет перехват, анализ и модификацию информации, передаваемой по линиям связи, проходящим вне контролируемой территории; осуществляет перехват и анализ электромагнитных излучений от оборудования ИС.

Предположения о квалификации внешнего нарушителя формулируются следующим образом:

является высококвалифицированным специалистом в области использования технических средств перехвата информации;

знает особенности системного и прикладного ПО, а также технических средств ИС;

знает специфику задач, решаемых ИС;

знает функциональные особенности работы системы и закономерности хранения, обработки и передачи в ней информации;

знает сетевое и канальное оборудование, а также протоколы передачи данных, используемые в системе;

может использовать только серийно изготовляемое специальное оборудование, предназначенное для съема информации с кабельных линий связи и из радиоканалов.

При использовании модели нарушителя для анализа возможных угроз ИБ необходимо учитывать возможность сговора между внутренними и внешними нарушителями.

Модель угроз информационной безопасности

Защита информационных компонентов и группы угроз

В качестве объектов защиты, рассматриваемых в рамках настоящей концепции, выступают следующие виды информационных ресурсов предприятия:

Информация (данные, телефонные переговоры и факсы) передаваемая по каналам связи.

Информация, хранимая в базах данных, на файловых серверах и рабочих станциях, на серверах каталогов, в почтовых ящиках пользователей корпоративной сети и т.п.

Конфигурационная информация и протоколы работы сетевых устройств, программных систем и комплексов.

Исходя из перечисленных свойств, все угрозы информационным ресурсам системы можно отнести к одной из следующих категорий:

Угрозы доступности информации, хранимой и обрабатываемой в ИС и информации, передаваемой по каналам связи;

Угрозы целостности информации, хранимой и обрабатываемой в ИС и информации, передаваемой по каналам связи;

Угрозы конфиденциальности информации хранимой и обрабатываемой в ИС и информации, передаваемой по каналам связи.

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

Угрозы, реализуемые с использованием технических средств;

Угрозы, реализуемые с использованием программных средств;

Угрозы, реализуемые путем использования технических каналов утечки информации.

Угрозы, реализуемые с использованием технических средств

Общее описание

Технические средства системы включают в себя приемо-передающее и коммутирующее оборудование, оборудование серверов и рабочих станций, а также линии связи. К данному

классу относятся угрозы доступности, целостности и, в некоторых случаях конфиденциальности информации, хранимой, обрабатываемой и передаваемой по каналам связи системы, связанные с повреждениями и отказами технических средств ИС, приемо-передающего и коммутирующего оборудования и повреждением линий связи.

Виды угроз

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

Вывод из строя (умышленный или неумышленный);

Несанкционированное либо ошибочное изменение конфигурации активного сетевого оборудования и приемо-передающего оборудования;

Физическое повреждение технических средств, линий связи, сетевого и каналообразующего оборудования;

Перебои в системе электропитания;

Отказы технических средств;

Установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты;

Хищение технических средств и долговременных носителей конфиденциальной информации вследствие отсутствия контроля над их использованием и хранением.

Источники угроз

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

стихийные бедствия;

пожар;

кража оборудования;

саботаж;

ошибки обслуживающего персонала;

терроризм и т. п.

Угрозы, реализуемые с использованием программных средств

Общее описание

Это наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов, связанный с получением НСД к информации, хранимой и обрабатываемой в системе, а также передаваемой по каналам связи, при

помощи использования возможностей, предоставляемых ПО ИС. Большинство рассматриваемых в этом классе угроз реализуется путем осуществления локальных или удаленных атак на информационные ресурсы системы внутренними и внешними злоумышленниками. Результатом успешного осуществления этих угроз становится получение НСД к информации БД и файловых систем корпоративной сети, данным, хранящимся на АРМ операторов, конфигурации маршрутизаторов и другого активного сетевого оборудования.

Виды угроз

В этом классе рассматриваются следующие основные виды угроз:

Внедрение вирусов и других разрушающих программных воздействий;

Нарушение целостности исполняемых файлов;

Ошибки кода и конфигурации ПО, активного сетевого оборудования;

Анализ и модификация ПО;

Наличие в ПО недекларированных возможностей, оставленных для отладки, либо умышленно внедренных;

Наблюдение за работой системы путем использования программных средств анализа сетевого трафика и утилит ОС, позволяющих получать информацию о системе и о состоянии сетевых соединений;

Использование уязвимостей ПО для взлома программной защиты с целью получения НСД к информационным ресурсам или нарушения их доступности;

Выполнение одним пользователем несанкционированных действий от имени другого пользователя («маскарад»);

Раскрытие, перехват и хищение секретных кодов и паролей;

Чтение остаточной информации в ОП компьютеров и на внешних носителях;

Ошибки ввода управляющей информации с АРМ операторов в БД;

Загрузка и установка в системе не лицензионного, непроверенного системного и прикладного ПО;

Блокирование работы пользователей системы программными средствами.

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

перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика;

замена, вставка, удаление или изменение данных пользователей в информационном потоке;

перехват информации (например, пользовательских паролей), передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации;

статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т. п.).

Источники угроз

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

Угрозы утечки информации по техническим каналам связи

Виды технических каналов утечки информации

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

побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;

акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;

несанкционированный доступ к информации, обрабатываемой в автоматизированных системах;

хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств.

Наибольшую опасность в настоящее время представляют технические средства разведки:

Акустическая разведка;

Разведка побочных электромагнитных излучений и наводок электронных средств обработки информации (далее - ПЭМИН);

В отдельных ситуациях, могут использоваться: телевизионная, фотографическая и визуальная оптическая разведка, обеспечивающая добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне электромагнитных волн с использованием телевизионной аппаратуры.

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

Радиоканалы;

ИК-канал;

Ультразвуковой канал;

Проводные линии.

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

сети переменного тока;

линии телефонной связи;

радиотрансляционные и технологические (пожарной, охранной сигнализации, кабели телеантенн и т.п.) линии;

специально проложенные проводные линии.

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

Источники угроз

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

Требования по обеспечению информационной безопасности

Требования к составу основных подсистем СОИБ

В состав СОИБ должны входить следующие подсистемы:

подсистема управления политикой информационной безопасности;

подсистема анализа и управления рисками;

подсистема идентификации и аутентификации;

подсистема разграничения доступа;

подсистема протоколирования и пассивного аудита;

подсистема активного аудита;

подсистема контроля целостности данных;

подсистема контроля защищенности;

подсистема удостоверяющий центр;

подсистема сегментирования ЛВС и межсетевого экранирования;

подсистема VPN;

подсистема антивирусной защиты;

подсистема фильтрации контента;

подсистема управления безопасностью;

подсистема предотвращения утечки информации по техническим каналам.

Требования к подсистеме управления политикой безопасности

Подсистема управления политикой ИБ предназначена для поддержания в актуальном состоянии политик и других организационно-распорядительных документов по обеспечению ИБ, ознакомление всех пользователей и технического персонала ИС с содержанием этих документов, контроля осведомленности и контроля выполнения требований политики безопасности и других регламентирующих документов. Всем сотрудникам предприятия предоставляется персонифицированный доступ к внутреннему информационному Web-серверу, на котором публикуются действующие нормативные документы, списки контрольных (проверочных) вопросов, предназначенных для контроля осведомленности, а также Web-формы для составления сообщений и отчетов об инцидентах, связанных с нарушением правил политики безопасности.

Подсистема управления политикой безопасности должна:

поддерживать, актуализировать и контролировать исполнение корпоративной политики безопасности;

обеспечивать определение единого набора правил обеспечения безопасности;

позволять создавать новые и модифицировать уже созданные политики, правила и инструкции для обеспечения информационной безопасности;

учитывать отраслевую специфику;

обеспечивать централизованный персонифицированный доступ сотрудников к текстам корпоративных политик на основе Web-доступа;

информировать пользователей о создании и утверждении новых политик;

фиксировать факт ознакомления пользователя с политиками;

проверять усвоенные знания политик;

контролировать нарушение политик пользователями;

контролировать выполнение единого набора правил защиты информации;

информировать административный персонал о фактах нарушения политик безопасности пользователями;

иметь средства создания отчетов.

Требования к подсистеме анализа и управления рисками

Подсистема анализа и управления рисками представляет собой комплекс инструментальных средств, установленных на рабочем месте специалиста по анализу рисков и предназначенных для сбора и анализа информации о состоянии защищенности ИС, оценки рисков, связанных с реализацией угроз ИБ, выбора комплекса контрмер (механизмов безопасности), адекватных существующим рисками и контроля их внедрения.

Подсистема анализа и управления рисками должна обеспечивать:

автоматизацию идентификации рисков;

возможность создания шкал и критериев, по которым можно измерять риски;

оценку вероятностей событий;

оценку угроз;

анализ допустимого уровня риска;

выбор контрмер и оценку их эффективности;

позволять контролировать необходимый уровень обеспечения информационной и физической безопасности (информационные риски, сбои в системах, служба охраны, охранно-пожарная сигнализация и пожаротушение, охрана периметра и т.п.).

Требования к подсистеме идентификации и аутентификации

Подсистема идентификации и аутентификации представляет собой комплекс программно-технических средств, обеспечивающих идентификацию пользователей ИС и подтверждение подлинности пользователей при получении доступа к информационным ресурсам. Подсистема идентификации и аутентификации включает в себя компоненты, встроенные в операционные системы, межсетевые экраны, СУБД и приложения, которые обеспечивают управление идентификационными данными пользователей, паролями и ключевой информацией, а также реализуют различные схемы подтверждения подлинности при входе пользователя в систему и получении доступа к системным ресурсам и приложениям. Встроенные средства идентификации и аутентификации дополняются наложенными средствами, обеспечивающими синхронизацию учетных данных пользователей в различных хранилищах (например, Active Directory, Lotus, Microsoft SQL, Novell Directory, LDAP, прикладные системы и т.п.) и предоставление единой точки доступа и администрирования для всех пользователей ИС.

Подсистема идентификации и аутентификации должна обеспечивать:

Поддержание идентичности и синхронизацию учетных данных в разных хранилищах (Active Directory, Lotus, Microsoft SQL, Novell Directory, LDAP, автоматизированные системы);

Комбинирование идентификационной информации из множества каталогов;

Обеспечение единого представления всей идентификационной информации для пользователей и ресурсов;

Предоставление единой точки доступа и администрирования;

Безопасный вход в домен ОС Windows (Windows-десктоп и сеть) при помощи электронного идентификатора (USB-ключа или смарт-карты);

Усиленную аппаратную двухфакторную аутентификацию пользователей (электронный идентификатор и пин-код);

Вход в сеть предприятия с любой рабочей станции, посредством хранения электронного сертификата в защищенной области памяти электронного идентификатора;

Хранение паролей к различным ресурсам (в том числе Web) и электронных сертификатов в защищенной области памяти электронного идентификатора

Централизованное управление данными об используемых электронных идентификаторах (USB-ключа или смарт-карты);

Блокирование компьютера или автоматическое отключение от сети в перерывах между работой и отсоединением электронного идентификатора.

Механизмы идентификации и аутентификации должны быть реализованы на всех рубежах защиты информации в следующих объемах:

На рубеже защиты внешнего периметра КСПД предприятия – идентификация и аутентификация внешних пользователей сети для доступа к информационным ресурсам ЛВС на МЭ и сервере удаленного доступа;

На рубеже сетевой инфраструктуры должна осуществляться идентификация и аутентификация пользовательских рабочих станций по именам и сетевым адресам при осуществлении доступа к сетевым сервисам ЛВС;

На рубеже защиты серверов и рабочих станций должна осуществляться идентификация и аутентификация пользователей при осуществлении локальной или удаленной регистрации в системе;

На рубеже прикладного ПО должна осуществляться идентификация и аутентификация пользователей указанного ПО для получения доступа к информационным ресурсам при помощи данного ПО.

Аутентификация внутренних и внешних пользователей системы осуществляется на основе следующей информации:

На рубеже защиты внешнего периметра для аутентификации пользователей на МЭ и сервере удаленного доступа используются схемы, устойчивые к прослушиванию сети потенциальными злоумышленниками, построенные на основе одноразовых сеансовых ключей и/или аппаратных носителей аутентификационной информации;

На рубеже защиты сетевых сервисов ЛВС используются параметры клиентов сетевого уровня (IP-адреса, имена хостов) в сочетании с параметрами канального уровня (MAC-адреса) и парольными схемами аутентификации;

На рубежах защиты серверов, рабочих станций и приложений используются парольные схемы аутентификации с использованием аппаратных носителей аутентификационной информации.

Требования к подсистеме разграничения доступа

Подсистема разграничения доступа (авторизации) использует информацию, предоставляемую сервисом аутентификации. Авторизация пользователей для доступа к информационным ресурсам ИС осуществляется на следующих уровнях программно-технической защиты:

На уровне защиты внешнего периметра ЛВС предприятия (при их подключении к внешним сетям и сети Интернет) МЭ осуществляет разграничение доступа внешних пользователей к сервисам ЛВС и внутренних пользователей к ресурсам сети Интернет и внешних сетей в соответствии с правилами «Политики обеспечения информационной безопасности при взаимодействии с сетью Интернет».

На уровне защиты сетевых сервисов ЛВС используются внутренние механизмы авторизации пользователей, встроенные в сетевые сервисы, либо специализированные серверы авторизации.

На уровне защиты серверов и рабочих станций ЛВС используются механизмы авторизации, встроенные в ОС, в сочетании с наложенными средствами разграничения доступа.

На уровне защиты приложений, функциональных подсистем ИС и системных ресурсов используются механизмы авторизации, встроенные в эти приложения, а также средства разграничения доступа ОС и СУБД.

Средства разграничения доступа должны исключать возможность доступа к ресурсам системы неавторизованных пользователей.

Требования к подсистеме протоколирования и пассивного аудита

Подсистема протоколирования и пассивного аудита предназначена для осуществления контроля за наиболее критичными компонентами сети, включающими в себя серверы приложений, баз данных и прочие сетевые серверы, межсетевые экраны, рабочие станции управления сетью и т.п. Компоненты этой подсистемы располагаются на всех перечисленных выше рубежах защиты (разграничения доступа) и осуществляют протоколирование, централизованный сбор и анализ событий, связанных с безопасностью (включая предоставление доступа, попытки аутентификации, изменение системных политик и пользовательских привилегий, системные сбои и т.п.). Они включают в себя как

встроенные средства, имеющиеся в составе ОС, СУБД, приложений и т.п. и предназначенные для регистрации событий безопасности, так и наложенные средства (программные агенты) служащие для агрегирования и анализа данных аудита, полученных из различных источников. Все данные аудита поступают на выделенный сервер аудита, где осуществляется их хранение и обработка. Просмотр и анализ этих данных осуществляется с консоли администратора аудита.

Подсистема пассивного аудита безопасности выполняет следующие основные функции:

Отслеживание событий, влияющих на безопасность системы;

Регистрация событий, связанных с безопасностью в журнале аудита;

Выявление нарушений безопасности, путем анализа данных журналов аудита администратором безопасности в фоновом режиме.

Средства протоколирования и аудита должны применяться на всех рубежах защиты в следующем объеме:

На рубеже защиты внешнего периметра должны протоколироваться следующие события:

Информация о состоянии внешнего маршрутизатора, МЭ, сервера удаленного доступа, модемов;

Действия внешних пользователей по работе с внутренними информационными ресурсами;

Действия внутренних пользователей по работе с внешними информационными ресурсами;

Попытки нарушения правил разграничения доступа на МЭ и на сервере удаленного доступа;

Действия администраторов МЭ и сервера удаленного доступа.

На рубеже сетевой инфраструктуры должно осуществляться протоколирование информации о состоянии структурированной кабельной системы (СКС) и активного сетевого оборудования, а также структуры информационного обмена на сетевом и транспортном уровнях;

На рубеже защиты серверов и рабочих станций средствами подсистем аудита безопасности ОС должно обеспечиваться протоколирование всех системных событий, связанных с безопасностью, включая удачные и неудачные попытки регистрации пользователей в системе, доступ к системным ресурсам, изменение политики аудита и т. п.;

На уровне приложений должна обеспечиваться регистрация событий, связанных с их функционированием, средствами этих приложений.

Эффективность функционирования системы пассивного аудита безопасности определяется следующими основными свойствами этой системы:

наличие средств аудита, обеспечивающих возможность выборочного контроля любых происходящих в системе событий, связанных с безопасностью;

наличие средств централизованного управления журналами аудита, политикой аудита и централизованного анализа данных аудита по всем контролируемым системам;

непрерывность контроля над критичными компонентами ЛВС во времени.

Требования к подсистеме активного аудита безопасности

Подсистема активного аудита безопасности предназначена для автоматического выявления нарушений безопасности критичных компонентов ИС и реагирования на них в режиме реального времени. К числу критичных компонентов ИС, с наибольшей вероятностью подверженных атакам со стороны злоумышленников, относится внешний защищенный шлюз в сеть Интернет, сервер удаленного доступа, серверная группа и рабочие станции управления сетью. Данная подсистема тесно интегрирована с подсистемой протоколирования и пассивного аудита, т.к. она частично использует данные аудита, полученные из этой подсистемы, для выявления атак и активизации алгоритмов автоматического реагирования.

Подсистема активного аудита строится на традиционной для подобных систем архитектуре агент-менеджер-управляющая консоль. Для сбора информации и реагирования на инциденты используются программные агенты, программа-менеджер размещается на сервере аудита и отвечает за агрегирование, хранение и обработку данных аудита, управление агентами и автоматическую активизацию алгоритмов реагирования. Управление всей подсистемой осуществляется с консоли администратора аудита.

Анализатор сетевого трафика должен обнаруживать известные типы сетевых атак, включая атаки, направленные против следующих приложений:

СУБД, Web, FTP, TELNET и почтовые серверы;

Серверы NIS, DNS, WINS, NFS и SMB;

Почтовые агенты и Web-браузеры;

Выявление сетевых и локальных атак и других нарушений безопасности, а также реагирование на них должны осуществляться в реальном времени.

Требования к подсистеме контроля целостности

Подсистема контроля целостности программных и информационных ресурсов ИС предназначена для контроля и оперативного восстановления целостности критичных файлов ОС и приложений на серверах и рабочих станциях сети, включая конфигурационные файлы, файлы данных, программы и библиотеки функций. Контроль целостности информационных ресурсов осуществляет путем регулярного подсчета контрольных сумм файлов и их сравнения с эталонной базой данных контрольных сумм. В случае несанкционированной модификации контролируемых файлов они могут быть

восстановлены с использованием средств резервного копирования и восстановления данных. Подсистема контроля целостности может входить в состав подсистемы активного аудита в качестве одного из ее функциональных компонентов.

Система контроля целостности программной и информационной части ЛВС должна обеспечивать контроль неизменности атрибутов критичных файлов и их содержимого, своевременное выявление нарушений целостности критичных файлов и их оперативное восстановление. В составе системы контроля целостности должны быть предусмотрены средства централизованного удаленного администрирования, средства просмотра отчетов по результатам проверки целостности и средства автоматического оповещения администратора безопасности о выявленных нарушениях.

Требования к подсистеме контроля защищенности

Подсистема контроля защищенности предназначена для выявления и ликвидации уязвимостей отдельных подсистем СОИБ, сетевых сервисов, приложений, функциональных подсистем, системного ПО и СУБД, входящих в состав ИС. Она включает в себя средства сетевого уровня (сетевые сканеры безопасности), устанавливаемые на рабочей станции администратора безопасности и предназначенные для выявления уязвимостей сетевых ресурсов путем эмуляции действий возможного злоумышленника по осуществлению удаленных атак, а также средства системного уровня, построенные на архитектуре «агент-менеджер-консоль» и предназначенные для анализа параметров конфигурации операционных систем и приложений, выявления уязвимостей, коррекции конфигурационных параметров и контроля изменения состояния операционных систем и приложений.

Сетевой сканер должен осуществлять сканирование всего диапазона TCP и UDP портов, выявлять все доступные сетевые ресурсы и сервисы, обнаруживать уязвимости различных ОС, СУБД, сетевых сервисов и приложений.

Средства анализа защищенности системного и прикладного уровней предназначены для решения следующих основных задач:

анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей, связанных с их некорректной настройкой, определения уровня защищенности контролируемых систем и соответствия политике безопасности организации;

коррекция конфигурационных параметров операционных систем и приложений;

контроль изменения состояния операционных систем и приложений, осуществляемый на основе мгновенных снимков их параметров и атрибутов файлов.

Средства контроля защищенности системного уровня должны выполнять проверки привилегий пользователей, политик управления паролями и регистрационных записей

пользователей, параметров подсистемы резервного копирования, командных файлов, параметров системы электронной почты, настройки системных утилит и т.п.

Средства контроля защищенности системного уровня должна поддерживать распределенные конфигурации и быть интегрированы с сетевыми сканерами и со средствами сетевого управления.

Требования к подсистеме «удостоверяющий центр»

Подсистема удостоверяющий центр предназначена для создания, распределения и управления цифровыми сертификатами пользователей ИС, ключами шифрования и ЭЦП. Она строится на инфраструктуре открытых ключей (PKI) и предоставляет базовые сервисы по управлению ключевой информацией для подсистемы аутентификации пользователей, средств VPN и подсистемы контроля целостности. На базе удостоверяющего центра стоятся системы электронного документооборота предприятия, включающие в себя защищенную электронную почту, внутренний информационный портал, офисные приложения и средства обмена документами в рамках подсистем судебного и общего делопроизводства.

Подсистема удостоверяющий центр должна поддерживать реализацию следующих функций:

электронно-цифровую подпись, контроль целостности информации и кодирование данных в рамках электронного документооборота (корпоративная система электронной почты, внутренний информационный портал, офисные приложения) на базе электронных сертификатов X.509;

кодирование данных и контроль целостности информации при передаче ее с помощью носителей информации и по открытым каналам в рамках * взаимодействия компонентов и пользователей информационной системы на базе электронных сертификатов X.509;

кодирование данных и контроль целостности информации при удаленном доступе мобильных сотрудников на базе электронных сертификатов X.509;

аутентификация пользователей и активного сетевого оборудования в рамках информационного взаимодействия на базе электронных сертификатов X.509

управление сервисом распределения электронных сертификатов;

безопасную транспортировку электронных сертификатов конечным пользователям;

поддержку жизненного цикла электронных сертификатов (генерация, распределение, отзыв, подтверждение);

поддержку хранения электронных сертификатов и паролей на внешних носителях (USB-токены, смарт-карты);

поддержка стандартов PKCS#11, PKCS#7.

Требования к подсистеме сегментирования и межсетевого экранирования

Подсистема сегментирования и межсетевого экранирования предназначена для разграничения межсетевого доступа на уровне сетевых протоколов и защиты ЛВС предприятия от сетевых атак со стороны сети Интернет и внешних сетей. В рамках системы должна быть сформирована и определена архитектура подключения к сетям общего пользования и создания демилитаризованной зоны (DMZ), которая может включать межсетевой экран, VPN-сервер, Web-сервер, транслятор (relay) электронной почты, вторичный кэширующий DNS-сервер, LDAP-сервер и подсистему защищенного удаленного доступа.

На рубеже сетевой инфраструктуры должны применяться средства сегментирования ЛВС. Средства сегментирования ЛВС должны строиться на технологии виртуальных ЛВС (VLAN) в соответствии с организационной структурой объединения и логикой работы подразделений предприятия с информационными ресурсами.

Серверы ЛВС должны быть расположены в выделенном сегменте (сегментах). Должно быть обеспечено отсутствие рабочих мест пользователей в указанных сегментах ЛВС.

На рубеже внешнего информационного обмена должны применяться средства межсетевого экранирования. Межсетевой экран должен обеспечивать фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях.

Требования к подсистеме VPN Подсистема VPN применяется на рубеже внешнего информационного обмена для защиты конфиденциальной информации, передаваемой между ЛВС различных удаленных офисов предприятия, которые не связаны между собой выделенными каналами, а также для подключения к ЛВС мобильных пользователей. Средства VPN реализуются на основе протокола IPSec и интегрируются со средствами межсетевого экранирования.

Средства VPN должны соответствовать спецификациям стандарта IPSec.

Средства VPN должны обеспечивать передачу данных как в зашифрованном, так и в открытом виде в зависимости от источника и получателя информации.

Средства VPN должны быть интегрированы с МЭ.

Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты сети предназначена для решения следующих задач:

Перекрытие всех возможных каналов распространения вирусов, к числу которых относятся: электронная почта, разрешенные для взаимодействия с сетью Интернет сетевые протоколы (HTTP и FTP), съемные носители информации (дискеты, CD-ROM и т.п.), разделяемые папки на файловых серверах;

Непрерывный антивирусный мониторинг и периодическое антивирусное сканирование всех серверов и рабочих станций, подключаемых к ЛВС;

Автоматическое реагирование на заражение компьютерными вирусами и на вирусные эпидемии, включающее в себя: оповещения, лечение вирусов, удаление троянских программ и очистку системы, подвергнувшейся заражению;

Она строится из следующих компонентов:

Средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;

Средства антивирусной защиты серверов ЛВС;

Средства антивирусной защиты рабочих станций;

Средства антивирусной защиты почтовой системы (внутренних почтовых серверов и SMTP-шлюзов на внешнем периметре сети);

Антивирусный шлюз, осуществляющий антивирусный контроль HTTP и FTP трафика.

Требования к подсистеме фильтрации контента

Подсистема фильтрации контента предотвращает утечку ценной конфиденциальной информации из ИС по протоколам HTTP, FTP и SMTP, осуществляет фильтрацию спама и прочей нежелательной корреспонденции. Она реализуется на рубеже защиты внешнего периметра сети и интегрируется со средствами межсетевого экранирования.

Подсистема фильтрации контента должна:

Предотвращать утечку ценной конфиденциальной информации из ЛВС по протоколам HTTP, FTP и SMTP путем ее блокирования и задержания до утверждения отправки руководством;

Обеспечивать увеличение производительности труда сотрудников путем уменьшения рекламы, рассылок и прочих, не имеющих отношения к делу, сообщений. Обнаружение спама, рассылаемого и получаемого сотрудниками предприятия;

Обеспечивать помощь в выявлении неблагонадежных сотрудников, рассылающих свои резюме и посещающих Web-сервера в поисках работы;

Обеспечивать контроль электронной почты, работающей через WEB-интерфейсы;

Обеспечивать контроль над всей выходящей корреспонденцией путем отсеивания сообщений, содержащих непристойное содержание для защиты репутации предприятия и

сотрудников путем предотвращения случайного или намеренного распространения писем непристойного содержания с адреса предприятия;

Обеспечивать русскоязычный поиск и фильтрацию почтовых сообщений;

Обеспечивать контроль использования корпоративного выхода в Internet в личных целях;

Разграничивать доступ сотрудников предприятия к ресурсам Internet и обеспечивать блокирование обращений к нежелательным сайтам.

В случае необходимости, осуществлять полное или частичное архивирование данных протоколов HTTP, FTP, SMTP.

Требования к подсистеме управления безопасностью

Подсистема управления безопасностью предназначена для осуществления централизованного управления всеми компонентами и подсистемами СОИБ. Управление всеми компонентами СОИБ осуществляется с консоли администратора безопасности, на которой устанавливаются соответствующие средства администрирования и мониторинга.

Средства управления безопасностью должны обеспечивать реализацию следующих функций:

управлять пользователями и ролями в кросс-платформенном окружении;

проверять, отслеживать, уведомлять в реальном времени и записывать изменения в групповых политиках безопасности;

устанавливать факт кем и когда были сделаны изменения параметров безопасности;

иметь средства, расширяющие встроенные возможности администрирования и управления безопасностью операционной системы;

иметь средства, управления парольной политикой – синхронизация, отслеживание истории изменений, распределение политики в кросс-платформенном окружении.

Доступ к элементам управления должен предоставляться только после обязательной процедуры аутентификации. Для аутентификации администраторов безопасности должны использоваться схемы, устойчивые к прослушиванию сети потенциальным злоумышленником.

С целью обеспечения реализации принципа минимизации административных полномочий, минимизации количества ошибочных и неправомерных действий со стороны администраторов ЛВС, должен быть определен, документирован, согласован и утвержден состав административных групп. При определении состава административных групп следует опираться на стандартный набор административных групп, имеющийся в ОС Windows 2003, а также в Windows XP.

Определение состава административных групп и выделенных им полномочий, а также порядка осуществления контроля над составом административных групп и действиями администраторов ЛВС должно содержаться в «Регламенте администрирования корпоративной сети». Каждой административной группе предоставляются только те полномочия, которые необходимы для выполнения задач администрирования определенных в Регламенте.

С целью упрощения задач управления доступом пользователей к ресурсам ЛВС назначение прав доступа осуществляется на уроне групп безопасности. Каждая пользовательская учетная запись входит в состав одной или нескольких групп в зависимости от принадлежности пользователя к тому или иному подразделению и его должностными обязанностями.

Требования к подсистеме предотвращения утечки информации по техническим каналам

Подсистема предотвращения утечки информации по техническим каналам предназначена для обеспечения защиты информации при ее обработке, хранении и передаче по каналам связи, а также конфиденциальной речевой информации, циркулирующей в специально предназначенных помещениях для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.). Она представляет собой совокупность организационно-технических мер по физической защите помещений, каналов передачи информации и технических средств, электромагнитной развязке между информационными цепями, по которым циркулирует защищаемая информация, развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров и другие меры защиты, предпринимаемые в соответствии с требованиями и рекомендациями нормативных документов.

При проведении работ по защите конфиденциальной речевой информации, циркулирующей в защищаемых помещениях, необходимо руководствоваться соответствующими требованиями СТР-К, направленными на исключение возможности перехвата конфиденциальной речевой информации в системах звукоусиления и звукового сопровождения кино- и видеофильмов, при осуществлении ее магнитной звукозаписи и передачи по каналам связи.

Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы контролируемой зоны, и радиоканалам должна быть исключена. При необходимости передачи информации следует использовать защищенные линии связи. Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

При защите конфиденциальной цифровой информации от утечки по техническим каналам необходимо руководствоваться следующими требованиями СТР-К:

использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

использование сертифицированных средств защиты информации;

размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;

размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах контролируемой зоны;

использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);

развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информативный сигнал;

электромагнитная развязка между информационными цепями, по которым циркулирует защищаемая информация, и линиями связи, другими цепями вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны;

использование защищенных каналов связи;

размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

организация физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации.

Технические требования к смежным подсистемам

Требования к структурированной кабельной системе

С точки зрения информационной безопасности при прокладке кабелей СКС необходимо иметь в виду следующее:

Открытая прокладка кабелей не допускается во избежание их механических повреждений. Механическое повреждение может привести как к обрыву линии, так и к ухудшению технических характеристик UTP-кабеля. Кроме того, механические повреждения приведут к аннулированию гарантии на компоненты.

Качество разделки кабеля на соединительных устройствах непосредственно влияет на излучающие свойства кабельной системы в целом. Таким образом, отклонения от правил заделки кабелей, указанных в стандарте EIA/TIA-568A, не допускаются.

Требования по физической защите

Физическая защита компонентов корпоративной сети должна представлять собой комплексную защиту помещений, персонала, аппаратуры, программ, данных, оборудования, зданий и прилегающей территории с использованием следующих средств:

Естественных особенностей объекта, ограждений, автоматических устройств сигнализации;

Внутренних и внешних датчиков, электронных средств поиска;

Замкнутой системы телевидения;

Системы оповещения и отображения;

Линий передачи данных, радио- и телефонной связи;

Управления безопасностью, оружия, транспорта, защитных средств;

Специальных входов и выходов из помещений, автоматической системы доступа, средств идентификации и проверки персонала;

Тренировок персонала системы защиты, проведения оперативных мероприятий, обследований, осуществления контроля доступа.

Надежная система физической защиты должна исключить:

Неправомочный доступ к аппаратуре обработки информации;

Неразрешенный вынос носителей информации;

Неправомочное использование систем обработки информации и незаконное получение данных;

Доступ к системам обработки информации посредством нестандартных (самодельных) устройств;

Неконтролируемое считывание, модификацию или удаление данных в процессе их передачи или транспортировки носителей информации.

Современный комплекс защиты территории охраняемых объектов должен включать следующие основные компоненты:

Механическая система защиты – механические конструкции, создающие для нарушителя реальное физическое препятствие;

Система оповещения о попытках вторжения – представляет собой систему тревожной сигнализации;

Система опознавания нарушителей – использует телевизионные установки дистанционного наблюдения;

Инфраструктура связи – проводные средства передачи информации, структурированные линии связи, оптико-волоконные системы, широкополосные радиомодемы и др.;

Центральный пост охраны - осуществляет сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;

Персонал охраны — патрули, дежурные на центральном посту

Ответственность сотрудников за нарушение безопасности

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности предприятия, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники предприятия несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

Механизм реализации концепции

Реализация Концепции обеспечения информационной безопасности предприятия должна осуществляться на основе утвержденных конкретных программ и планов, которые ежегодно уточняются с учетом:

федерального законодательства и нормативной базы в области защиты информации;

международных и отраслевых стандартов в области информационной безопасности и IT-безопасности;

организационно-распорядительных документов предприятия;

реальных потребностей в средствах обеспечения информационной безопасности;

объемов финансирования, выделяемых на обеспечение информационной безопасности предприятия.