Министерство образования и науки РФ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина»
Институт фундаментального образования
Кафедра интеллектуальных информационных технологий

К ЗАЩИТЕ ДОПУСТИТЬ

Заведующий кафедрой ИИТ

_____И. Н. Обабков

« ____»_____20___ г.

СИСТЕМА УПРАВЛЕНИЯ IT-СЕРВИСАМИ. ПОДСИСТЕМА УПРАВЛЕНИЯ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЕЙ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Пояснительная записка

Руководитель

Консультант

Консультант

Нормоконтролер

Студент гр. ФОМ–201101

Екатеринбург – 2015

Обозначения и сокращения

ИБ – информационная безопасность

ПДн – персональные данные

ИСПДн – информационная система персональных данных

УБПДн – угрозы безопасности персональных данных

СЗПДн – средство защиты персональных данных

АС – автоматизированная система

ИС – информационная система

АРМ – автоматизированное рабочее место

ПЭМИ – побочное электромагнитное излучение

ИР – информационные ресурсы

ПО – программное обеспечение

СЗИ – средство защиты информации

СКЗИ – средство криптографической защиты информации

ЛВС – локальная вычислительная сеть

СВТ – средства вычислительной техники

ДМЗ – демилитаризованная зона

НСД – несанкционированный доступ

КЗ – контролируемая зона

ОРД – организационно-распорядительная документация

ФСБ России – Федеральная служба безопасности

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

Содержание

Введение.....5
Глава 1. Анализ информационной системы.....7
1.1 Описание предприятия.....7
1.2 Схема системы документооборота.....8
1.3 Структура и особенности сети предприятия.....9
1.4 Информационные ресурсы.....11
Глава 2. Разработка частной модели угроз.....14
2.1 Описание ИСПДн.....14
2.1.1 Организация физической безопасности объектов (охрана).....14
2.1.2 Описание объектов безопасности, требующих защиты.....15
2.2 Анализ и классификация источников угроз информации, циркулирующей на объекте. 19
2.3 Модель нарушителя.....18
2.3.1 Внешние нарушители.....20
2.3.2 Внутренние нарушители.....21
2.4 Анализ предполагаемой квалификации нарушителя.....21
2.5 Определение актуальных угроз безопасности ПДн в ИСПДн.....23
2.5.1 Расчет исходной защищенности.....25
2.6 Частная модель угроз.....31
Глава 3. Разработка политики информационной безопасности и организационно-распорядительной документации.....32
3.1 Правовая основа обеспечения ИБ предприятия.....32
3.2 Цели обеспечения безопасности информации на предприятии.....33
3.3 Цели и задачи политики информационной безопасности.....34
3.4 Порядок внутреннего анализа рисков.....34
3.4.1 Аудит информационной безопасности.....34
3.5 Должностные обязанности администраторов.....35
3.5.1 Обязанности администратора информационной безопасности.....36

3.5.2 Обязанности системного администратора.....36
3.6 Планирование мероприятий по информационной безопасности для компонент автоматизированной системы.....37
3.6.1 Предпроектная стадия.....38
3.6.2 Стадия разработки/приобретения.....38
3.6.3 Стадия установки.....39
3.6.4 Стадия функционирования и поддержки.....40
3.6.5 Стадия списания.....40
3.7 Физическая безопасность.....41
3.7.1 Защита центров данных и компьютерных залов.....43
3.7.2 Правила использования рабочего стола.....44
3.7.3 Источники электропитания.....45
3.7.4 Защита оборудования, используемого за пределами предприятия.....46
3.8 Технические средства.....46
3.8.1 Требования к подсистеме идентификации.....46
3.8.2 Требования к подсистеме аутентификации.....47
3.8.3 Требования к парольной подсистеме.....48
3.8.4 Требования к системам регистрации сетевых событий.....50
3.9 Функциональные средства.....51
3.9.1 Работа с персоналом.....51
3.9.2 Планирование непрерывной работы.....52
3.9.3 Средства поддержки программных приложений.....52
3.9.4 Средства обеспечения целостности информации.....53
3.9.5. Документирование.....55
3.9.6. Осведомлённость и обучение специалистов.....55
3.9.7 Действия в случаях возникновения происшествий.....56
Заключение.....57
Список используемой литературы.....59
Приложения.....61

Введение

Актуальность работы. Обеспечение информационной безопасности на сегодняшний день выступает в качестве одного из самых главных требований к информационным системам. Причиной этому служит наличие неразрывной связи между информационными технологиями и основными бизнес-процессами во всех организациях, будь то государственная служба, промышленное предприятие, финансовая структура, операторы телекоммуникаций.

Обеспечить внутреннюю информационную безопасность - не только российская, но и общемировая проблема. В первые годы внедрения корпоративных локальных сетей основная головная боль компании заключалась в несанкционированном доступе к коммерческим данным путем внешнего взлома (хакерская атака), на сегодняшний день с этой проблемой успешно справляются. Во всех IT-отделах крупных уважающих себя компаний, как правило, имеется обширное число антивирусов, которые ограждают программы (файрволы) и другие средства борьбы с внешними атаками. Так, достижения российских программистов в вопросах обеспечения внешней безопасности достаточно велики - отечественные антивирусы по праву считаю одними из лучших в мире.

С позиции информационной безопасности множество современных компаний имеют вид крепостей, окруженных несколькими мощными стенами. Однако исходя из практики, все равно происходит утечка информации. Так, становится явной необходимость создания эффективных и экономически выгодных систем безопасности информационных систем предприятия.

Для повышения осведомленности пользователей в области рисков, связанных с информационными ресурсами и для определения степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности на предприятии было решено разработать политику информационной безопасности и организационно-распорядительную документацию в области информационной безопасности для предприятия ФКУ

«Налог-Сервис» ФНС России в Тюменской области.

Целью дипломной работы является разработка политики информационной безопасности и организационно-распорядительной документации в области информационной безопасности для предприятия ФКУ «Налог-Сервис» ФНС России в Тюменской области.

Целью дипломного проекта является совершенствование системы защиты информации в ФКУ «Налог-Сервис».

Объектом дипломного проектирования является – технология обеспечения информационной безопасности, а предметом дипломного проектирования – информационная безопасность предприятия.

Для достижения поставленной цели были выделены следующие задачи:

- анализ информационной системы;
- анализ и классификация источников угроз информации;
- разработка частной модели угроз информационной безопасности;
- разработка политики информационной безопасности;
- разработка регламентов, положений и инструкций в области информационной безопасности.

Теоретическую и методологическую основу данной работы составляют труды, выполненные отечественными и зарубежными учеными в сфере безопасности информационных систем. Особая роль отводится законодательным актам и нормативным документам Российской Федерации, периодическим изданиям, учетным и отчетным данным организации. В ходе разработки и решения поставленных задач были применены такие методы, как наблюдение, группировка, сравнение, обобщение, абстрактно-логическое суждение и др.

Глава 1. Анализ информационной системы

1.1 Описание предприятия

ФКУ «Налог-Сервис» ФНС России в Тюменской области (ФКУ «Налог-Сервис») создано для уменьшения объема ручных операций и сроков обработки информации, максимальной автоматизации процедур налогового администрирования, а также централизации информационных ресурсов на федеральном уровне, что даст возможность значительно улучшить качество обслуживания налогоплательщиков.

Основной целью деятельности предприятия является организационно-техническое и информационное обеспечение деятельности Федеральной налоговой службы России и ее территориальных органов, в пределах полномочий, переданных от ФНС России.

ФКУ «Налог-Сервис» осуществляет администрирование технического, программного и информационного обеспечения автоматизированной информационной системы ФНС России (АИС Налог).

Основные виды деятельности ФКУ «Налог-Сервис»:

- централизованный ввод в систему электронной обработки данных (ЭОД) данные, поступившие в налоговую инспекцию на бумажном носителе или в электронном виде по каналам связи, а это: налоговые декларации и бухгалтерская отчетность;
- ввод сведений по иным документам, поступающим в налоговые инспекции, а также ввод сведений, получаемых ИФНС на плановой основе в соответствии со статьей 85 Налогового Кодекса РФ. Это сведения об имуществе, земельных участках, сведения кадастрового учета, паспортные данные лиц и многие другие. (Полный перечень этих сведений можно посмотреть в ст. 85 НК);
- большое количество документов истребуется налоговыми органами. Двойное истребование (повторное у одного и того же плательщика) на данный момент запрещено, поэтому сотрудники вводят сведения об

истребованных документах в систему ЭОД и в центр обработки данных, чтобы исключить повторное истребование. Это касается таких документов, как: счета-фактуры, книги покупок/продаж, выписки банков и другие, которые получены налоговыми органами в результате процедуры истребования;

- централизованная печать и/или массовая рассылка налогоплательщикам налоговых документов по имущественным налогам, в т.ч. в электронном виде по телекоммуникационным каналам связи;
- централизованное архивное хранение в бумажном и электронном виде документов, поступающих или образующихся в результате деятельности налоговых органов;
- формирование архивных фондов, осуществление учета, хранения научно-технической обработки архивных документов, образовавшихся в результате деятельности налоговых органов;
- обеспечение мероприятий по защите информации.

1.2 Схема системы документооборота

Общая схема циркуляции информации в системе документооборота представлена на Рисунке1.1.

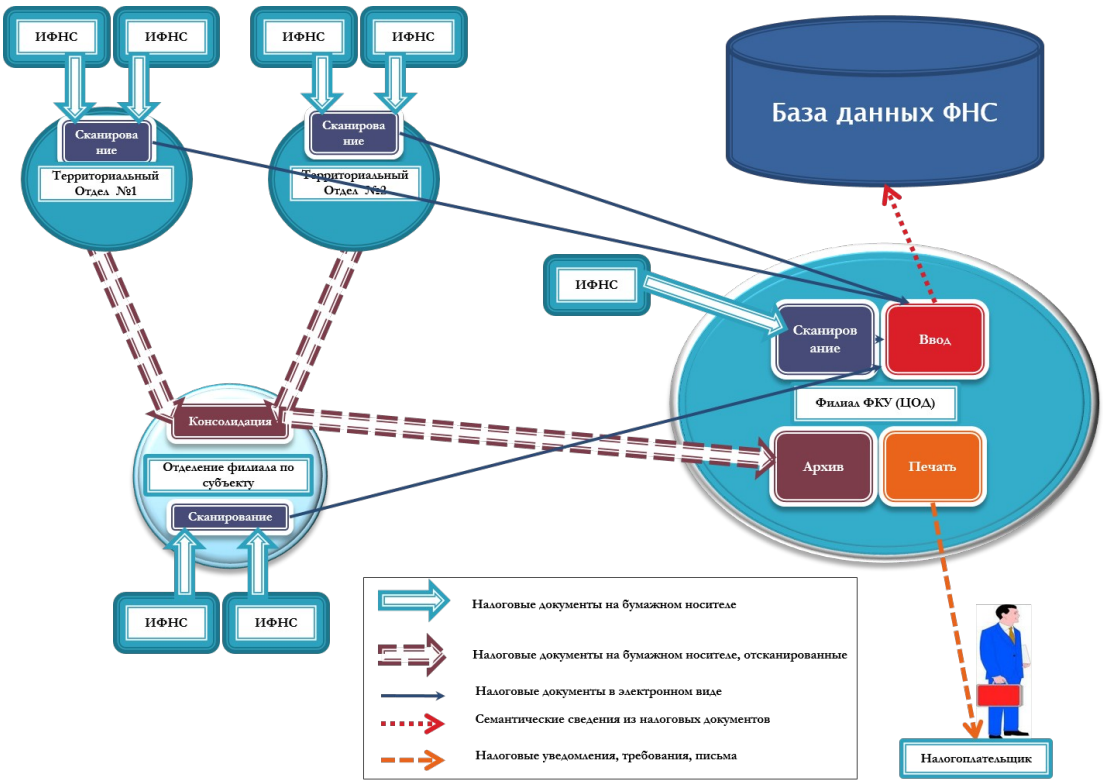

Рисунок 1 - общая схема циркуляции информации в системе документооборота

1.3 Структура и особенности сети предприятия

Рассмотрим структуру и особенности сети предприятия (рис. 2):

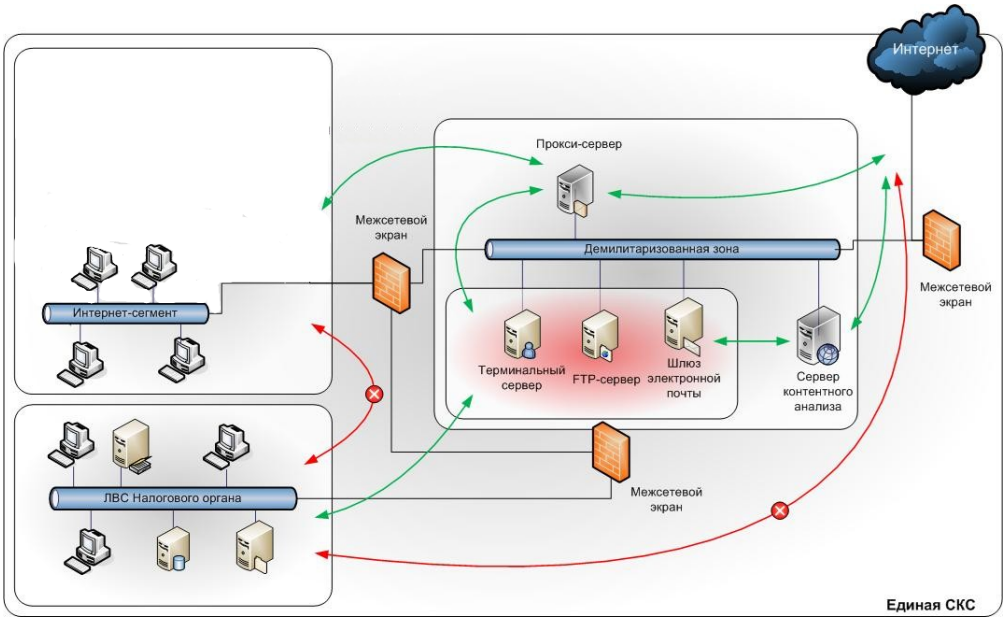

Рисунок 2 - структура сети предприятия

Внутренний сегмент ЛВС – сегмент (или совокупность сегментов) ЛВС налогового органа, в котором расположены сервера и рабочие станции пользователей, на которых обрабатывается информация ограниченного доступа или которые взаимодействуют с компонентами автоматизированной системы (АС), на которых такая информация обрабатывается.

Интернет-сегмент ЛВС – сегмент ЛВС налогового органа, в котором расположены рабочие станции пользователей и, возможно, сервера, на которых не обрабатывается информация ограниченного доступа и которые не взаимодействуют с компонентами АС, на которых такая информация обрабатывается.

Демилитаризованная зона (ДМЗ) – сегмент (или совокупность сегментов) ЛВС налогового органа, в котором расположены компоненты АС, взаимодействующие с сетью Интернет.

Ключевые особенности сети:

- Локальная вычислительная сеть (ЛВС) налогового органа и Интернет-сегмент реализованы в различных структурированных кабельных системах (СКС);
- Подключение к сети Интернет ЛВС налогового органа допускается осуществлять только с использованием средств шифрования трафика (в виде VPN-туннеля);
- Взаимодействие между внутренним сегментом ЛВС и интернет-сегментом запрещено;
- Взаимодействие между внутренним сегментом ЛВС и сетью Интернет запрещено;
- Специальных ограничений на взаимодействие между интернет-сегментом и демилитаризованной зоной не накладывается;
- Взаимодействие между внутренним сегментом ЛВС и демилитаризованной зоной допускается только по протоколу терминального соединения (для установления связи с терминальным сервером доступа в сеть Интернет), протоколу FTP (для передачи файлов из ДМЗ на рабочую станцию

пользователя) и почтовым протоколам.

1.4 Информационные ресурсы

Объектом защиты являются информационные ресурсы (ИР) налоговых органов (библиотеки, архивы и фонды; банки, базы и файлы данных; отдельные документы на традиционных носителях), содержащие зафиксированные на материальном носителе (независимо от его формы) сведения, используемые в процессе сбора, обработки, накопления, хранения, распространения, взаимодействия в рамках исполнения возложенных на ФКУ «Налог-Сервис» функций.

1. К ИР ФКУ «Налог-Сервис», содержащим информацию ограниченного доступа (распространения) относится информация конфиденциального характера:

- Налоговые ИР - ресурсы по государственной регистрации налогоплательщиков; содержащие полученные налоговыми органами сведения о налогоплательщиках: охраняемые налогоплательщиком сведения о производственной деятельности и коммерческой деятельности (ресурсы: «Недействительные паспорта», «Банковские счета», НДС, «Налоговая отчетность по форме 7-НП», «Сведения о физических лицах», частично: «ЕГРИП», «ЕГРЮЛ» в части сведений о номере документа, о дате выдачи и об органе, выдавшем документ, удостоверяющий личность физического лица и т.д.);
- ИР персональных данных - ресурсы, содержащие сведения, составляющие персональные данные работников налоговых органов (ресурсы: «Бухгалтерия», «Кадры», «Бюро пропусков» и другие);
- Служебные ИР - ресурсы, содержащие сведения, необходимые для обеспечения работы информационно-аналитической системы ФКУ «Налог-Сервис», в том числесведения, составляющие служебную тайну взаимодействующих с ФКУ «Налог-Сервис»органов государственной власти;

- Технологические ИР - ресурсы, содержащие сведения о принципах, методах, технических решениях и правилах обеспечения безопасности информации в ФКУ «Налог-Сервис» и ее территориальных органах;
- ИР ключевых систем информационной инфраструктуры.

Защита ИР, содержащих информацию ограниченного доступа (распространения), представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации;
- реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

2. К ИР, содержащих открытую информацию, которые подлежат защите от уничтожения, модифицировании, блокирования, а также от иных неправомерных действий в отношении такой информации, и на реализацию права на доступ к информации относятся:

- Открытые налоговые ИР – ресурсы, содержащие сведения о нарушениях законодательства о налогах и сборах, и мерах ответственности за эти нарушения, а также сведения, передаваемые средствам массовой информации, в соответствии с законодательством Российской Федерации;
- Базовые государственные ИР – ресурсы, содержащие сведения, по реализации государственной услуги, по регистрации юридических лиц и индивидуальных предпринимателей, а также ресурсы, подключаемые к единой системе межведомственного электронного взаимодействия (ресурсы: «ЕГРН», «ЕГРИП», «ЕГРЮЛ» (за исключением сведений, отнесенных к информации ограниченного доступа);
- Общедоступные ИР – ресурсы, содержащие информацию о деятельности налоговых органов в соответствии Федеральным законом № 8-ФЗ

«Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Защита Открытых ИР представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от уничтожения, модифицирования, блокирования, а также от иных неправомерных действий в отношении такой информации;
- реализацию права каждого на доступ к информации.

Глава 2. Разработка частной модели угроз

2.1 Описание ИСПДн

ИСПДн предприятия представляет собой распределенную информационную систему, состоящую из рабочих станций и серверов. ИСПДн имеет подключения к сетям связи общего пользования. Обработка ПДн производится в многопользовательском режиме с разграничением прав доступа, речевая обработка ПДн не производится. Технические средства ИСПДн находятся в пределах Российской Федерации.

В ИСПДн одновременно обрабатываются данные менее 1000 субъектов, которые позволяют идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением 1 категории персональных данных.

Для объектов защиты ИСПДн установлены следующие характеристики безопасности:

- конфиденциальность;
- целостность;
- доступность.

Осуществляется взаимодействие с информационными системами:

- Федеральной налоговой службы;
- Пенсионного фонда РФ;
- Фонда социального страхования;
- Трудовой инспекции;
- Федеральной миграционной службы;
- Кредитно-финансовых организаций (банки).

2.1.1 Организация физической безопасности объектов (охрана)

Охрана осуществляется круглосуточным постом на входе в охраняемую территорию компании. Режим входа работников в организацию - по

персональным идентификационным карточкам доступа или на основании служебного удостоверения. Пребывание посетителей осуществляется в сопровождении работника предприятия. В организации действует охранно-пожарная сигнализация. Во всех кабинетах установлены пожарные и охранные датчики различных типов. Ведется видеонаблюдение.

2.1.2 Описание объектов безопасности, требующих защиты

Таблица 1 - Содержание объектов защиты для ИСПДн предприятия

Описание объекта безопасности	**Примечание**
ПДн в виде акустических (речевых) сигналов. Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.	В организации не производится голосовая обработка ПДн.
ПДн на средствах отображения графической, видео- и буквенно-цифровой информации. Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.	В организации применяются СВТ, обрабатывающие видовую информацию: мониторы АРМ и серверов.
ПДн в виде побочных информативных электромагнитных полей и электрических	В ИСПДн применяются средства вычислительной техники, обладающие

Описание объекта безопасности	Примечание
сигналов. Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.	свойствами излучения ПЭМИ: (системные блоки, мониторы и т.п.).
АРМ пользователя ИСПДн. АРМ пользователей являются технической частью ИСПДн, через которые возможна реализация различных видов атак.	В ИСПДн имеются рабочие станции пользователей, на которых производится обработка персональных данных.
Серверы ИСПДн. Серверы ИСПДн обрабатывают наибольшие объемы конфиденциальной информации и являются объектом различных угроз и атак.	В ИСПДн имеются серверы, на которых производится обработка персональных данных.
Базовая система ввода-вывода АРМ пользователя или сервера. Несанкционированный доступ базовой системе ввода/вывода (BIOS) дает возможность перехвата управления загрузкой операционной системы и получения прав доверенного пользователя.	Применяемые в ИСПДн средства вычислительной техники включают в свою архитектуру базовую систему ввода/вывода.
Атрибуты безопасности (логины, пароли), данные, содержащие аутентификационную информацию. Аутентификационные данные являются наиболее критичной в плане безопасности информацией.	В ИСПДн применяются методы идентификации и аутентификации пользователей ИСПДн, с целью обеспечения санкционированного доступа к конфиденциальной информации.
Общесистемное или прикладное ПО. Угрозы, связанные с получением несанкционированного доступа к ПО, дают возможность нарушения основных характеристик безопасности информации.	В ИСПДн используется следующее основное ПО: - Microsoft SQL Server - Microsoft Windows Server 2008 - Microsoft Windows Server 2003

Описание объекта безопасности	Примечание
	- Microsoft Windows XP Pro RU - 1С 8.2 Конфигурация "Зарплата и управление персоналом" - Microsoft Windows Server Standart 2003 R2 - 1С Бухгалтерия+Зарплата и кадры 8.0 - Microsoft SQL Server 2005 - Kaspersky Business Space Security Russian Edition
Технические средства ИСПДн. Технические средства ИСПДн подвержены угрозам утечки информации по техническим каналам, а также другим угрозам нарушения основных характеристик безопасности информации.	В ИСПДн используются современные общепринятые технические средства: персональные компьютеры, мониторы, ноутбуки, принтеры, сканеры, копиры, факсы, телефоны и т.п.
ПДн, иная конфиденциальная информация на бумажных носителях. Конфиденциальная информация, обрабатываемая не автоматизированным способом, во избежание нанесения ущерба субъектам ПДн, должна защищаться.	В ИСПДн возможна обработка ПДн сотрудников организации на бумажных носителях.
Состав, маршрутно-адресная информация, сетевые службы и некоторые иные характеристики сети и ее узлов. Информация об сетевой инфраструктуре конфиденциальна. Цель – снижение вероятности реализации сетевых атак и других угроз, использующих уязвимости ЛВС.	
Носители информации с ПДн. Все носители конфиденциальной информации, используемые в организации должны быть учтены в установленном порядке. Характер	В организации могут использоваться различные виды носителей: диски, их массивы, флэш-карты, бумажные носители.

Описание объекта безопасности	Примечание
работы с ними должен находиться под контролем ответственных лиц.	
Списываемые технические средства ИСПДн, носители информации. Списываемые технические средства могут содержать остаточную конфиденциальную информацию, данные о ИСПДн и способах ее защиты. Процедуры утилизации должны быть регламентированы и выполняться под контролем ответственных лиц.	В организации организовано плановое обновление технических средств на более современные.
Персонал организации. Сотрудники организации могут попасть под воздействие со стороны злоумышленника, могут нанести вред субъектам ПДн по неосторожности или самостоятельно преследовать корыстные цели. Поэтому работа с персоналом по линии информационной безопасности является наиболее актуальной.	Доступ к элементам ИСПДн имеют сотрудники, обрабатывающие персональные данные, а также обеспечивающие функционирование системы.

2.2 Анализ и классификация источников угроз информации, циркулирующей на объекте

При анализе и классификации источников угроз информации, циркулирующей на объекте исходим из предположения, что для одной и той же угрозы методы отражения для внешних и внутренних источников могут быть разными.Особую группу внутреннихисточников составляют специально внедрённые и завербованные агенты из числа вспомогательного, основного, технического персонала и представителей отдела информационной безопасности.

Было решено разделить все источники угроз безопасности информации на три основные группы:

– антропогенные источники угроз (ошибки эксплуатации, ошибки проектирования и разработки компонентов АС,преднамеренные действия нарушителей и злоумышленников;

– техногенные источники угрозы (аварии, сбои и отказы оборудования (технических средств));

– обусловленные стихийными источниками (стихийные бедствия, катаклизмы).

Таким образом, классификация и перечень источников угроз присущих объекту информатизации представлены Таблицах 2; 3

Таблица 2 - Антропогенные источники угроз

№ п/п	Внешние антропогенные источники	№ п/п	Внутренние антропогенные источники
1.	Криминальные группы и отдельные преступные субъекты	1.	Работники предприятия (Основной персонал)
2.	Потенциальные преступники (недобросовестные налогоплательщики) и хакеры	2.	Администраторы АС, ЛВС, ТКУ, Администратор безопасности, программисты, администратор домена
3.	Персонал поставщиков телематических услуг (Провайдеры)	3.	Технический персонал
4.	Представители надзорных организаций и аварийных служб	4.	Работники отдела безопасности

В качестве антропогенных источников угрозвыступают субъекты, имеющие санкционированный/несанкционированный доступ к работе со штатными средствами объекта информатизации, действия которых могут быть распознаны, как умышленные или совершенные по неосторожности. Данная группа источников угроз представляет наибольший интерес, так как действия субъекта всегда можно оценить, спрогнозировать, и принять соответствующие меры.Контрмеры в этом случае напрямую зависят от действий организаторов информационной безопасности.

Таблица 3 - Техногенные источники угроз

№ п/п	Внешние техногенные источники угроз	№ п/п	Внутренние техногенные источники угроз
1.	Средства связи, промышленные установки ионизирующего излучения, системы энергообеспечения	1.	Некачественные технические средства обработки информации
2.	Сети инженерных коммуникаций (водоснабжения, канализации)	2.	Некачественные программные средства обработки информации
3.	Транспорт (авиационный, железнодорожный, автомобильный, водный)	3.	Вспомогательные средства (охраны, сигнализации, телефонии, видеонаблюдения, СКУД)
		4.	Другие технические средства, применяемые на предприятии

Техногенные источники угроз характеризуются технократической деятельностью человека и развитием техники.

Группа стихийных источников угроз объединяет обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех, которые невозможно предусмотреть или предотвратить,или возможно предусмотреть, но невозможно предотвратить. Защитные меры от стихийных источников угроз должны применяться всегда, т.к. их невозможно спрогнозировать. Стихийные источники угроз информационной безопасностипо отношению к защищаемому объекту, как правило, являются.

2.3 Модель нарушителя

Все нарушители делятся на две основные группы: внутренние и внешние. Под внутренними нарушителями подразумеваются все работники объекта информатизации, имеющие санкционированный доступ на территорию объекта к ресурсам автоматизированной системы (АС). Под внешними нарушителями подразумеваются все остальные лица.

2.3.1 Внешние нарушители

– лица, самостоятельно создающие методы и средства реализации атак, а также самостоятельно реализующие атаки, совершающие свои действия с целью нанесения ущерба;

– поставщики программного обеспечения и технических средств (могут владеть информацией о структуре сети, недекларированных возможностях оборудования и программного обеспечения).

Внешние нарушители могут знать организационно-техническую структуру объекта информатизации, и быть, в том числе, бывшими работниками.

2.3.2 Внутренние нарушители

– пользователь информационных ресурсов объекта информатизации;

– обслуживающий персонал (системные администраторы, администраторы АС, администраторы баз данных, инженеры);

– работники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;

– другие работники структурных подразделений, имеющие санкционированный доступ на объект информатизации, где расположено оборудование передачи и обработки информации.

Возможности внутреннего нарушителя зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

Таблица 4 - Описание модели нарушителя для ИСПДн предприятия.

№ п/п	Описание нарушителя	По методике ФСТЭК	Описание (пример)
1	Лица, не имеющие права доступа в контролируемую зону информационной системы	Внешний	Разведывательные службы государств, криминальные структуры, конкуренты, недобросовестные партнеры, внешние субъекты (физические лица).
2	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн	Категория 1	Директор филиала; Отдел системного администрирования,
3	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места	Категория 2	Все пользователи информационной системы ФКУ «Налог-Сервис»
4	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	Категория 3	-
5	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн	Категория 4	-
6	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн	Категория 5	-
7	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	Категория 6	-
8	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	Категория 7	-
9	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	Категория 8	-

2.3 Анализ предполагаемой квалификации нарушителя

Анализ предполагаемой квалификации потенциального нарушителя проводится по классификационным признакам. Кто бы ни был источником нарушения, какое бы оно не было, все нарушители имеют одну общую черту - доступ к объекту информатизации.

Применительно к конкретным условиям функционирования объекта информатизации уровень технической подготовки потенциального нарушителя, его квалификацию необходимо ранжировать следующим образом:

- не является специалистом в области вычислительной техники;
- самый низкий уровень возможностей – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации;
- возможности создания и запуска собственных программ с новыми функциями по обработке информации;
- возможность управления функционированием автоматизированной системы, т.е. воздействием на базовое программное обеспечение системы, на конфигурацию ее оборудования;
- включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав АС собственных технических средств с новыми функциями по обработке информации.

Внешний нарушитель не имеет непосредственного доступа к штатным средствам объекта информатизации, зачастую действует в сговоре с внутренним нарушителем. Нарушитель может использовать пассивные и/или активные методы вторжения в АС.

При пассивном вторжении нарушитель использует каналы утечки информации, не нарушая информационный поток и не влияет на содержание информации. Он наблюдает за прохождением информации по информационно-телекоммуникационной сети. Пассивное вторжение опасно при несоблюдении специальных требований и рекомендаций по защите конфиденциальной

информации. Пассивное вторжение всегда связано только с нарушением конфиденциальности информации, т.к. при этом никаких действий с объектами доступа не производится.

При активном вторжении нарушитель стремится подменить, исказить или уничтожить информацию, передаваемую по информационно-телекоммуникационной сети, получить удаленный доступ к информационным ресурсам АС, преодолев систему разграничения доступа, оказывает воздействие на персонал объекта информатизации. По каналам передачи данных он может выборочно модифицировать, удалить, задержать или изменить порядок следования сообщений, пытаться подобрать пароли. Активное вторжение осуществляется с использованием методов несанкционированного доступа (НСД).

В качестве внутреннего нарушителя на объекте информатизации рассматривается субъект, имеющий доступ к работе со штатными средствами объекта. Внутренний нарушитель имеет возможность непосредственного доступа к материальным носителям информации, к средствам автоматизированной обработки данных. Внутренние нарушители характеризуются по уровню возможностей, предоставляемых им штатными средствами.

Применительно к объекту информатизации, внутренних нарушителей можно разделить на группы:

– пользователи информационных ресурсов (госналогинспектора, бухгалтеры, сотрудники кадровых аппаратов и другие пользователи, работающие с узким кругом прикладного программного обеспечения);

– обслуживающий персонал (администраторы АС, ЛВС, ТКУ, администраторы безопасности СКЗИ, сотрудники отдела безопасности осуществляющие настройку и эксплуатацию средств защиты информации, в том числе криптографической);

– сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение, администраторы баз данных;

– другие работники подразделений объекта информатизации, имеющие санкционированный доступ на объект, где расположено оборудование передачи и обработки информации АС.

Первые две группы по уровню возможностей относятся к пользователям, допущенным к обработке информации в АС, последние две относятся к работникам наделенными полномочиями по администрированию и обслуживанию АС. Однако не исключается возможность, что внутренний нарушитель, воспользовавшись недекларированными возможностями установленного программного обеспечения, может повысить свои полномочия.

2.4 Определение актуальных угроз безопасности ПДн в ИСПДн

При определении актуальности угроз и их описании используются два методических документа, разработанных и утвержденных ФСТЭК России:

– Базовая модель угроз безопасности ПДн при их обработке в ИСПДн;

– Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн.

2.4.1 Расчет исходной защищенности

В таблице 5 представлена информация по расходу исходной защищенности ИСПДн предприятия.

Таблица 5 - Расход исходной защищенности ИСПДн предприятия

Показатели защищенности	Уровень защищенности		
Технические и эксплуатационные характеристики ИСПДн	Высокий	Средний	Низкий
По территориальному размещению:			
распределеннаяИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городскаяИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальнаяИСПДн, развернутая в пределах одного здания	+	–	–
По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДнИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю	+	–	–

Показатели защищенности	Уровень защищенности		
Технические и эксплуатационные характеристики ИСПДн	Высокий	Средний	Низкий
данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–
Итого для ИСПДн Филиала, (%)	14%	29%	57%

ИСПДн имеет низкий уровень исходной защищенности и соответственно коэффициент Y_1 равен 10.

По итогам оценки уровня защищенности Y_1 и вероятности реализации угрозы Y_2, рассчитывается коэффициент реализуемости угрозы Y и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.

Анализ рисков производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера.

Цель анализа рисков заключается в определении характеристик рисков АС и её ресурсов. Результаты анализа рисков используются в рамках мероприятий по экспертизе средств защиты как один из критериев оценки уровня защищённости АС.

При проведении анализа рисков учитываются следующие основные факторы:

- ценность программно-аппаратных и информационных ресурсов автоматизированной системы;

- значимость угроз и уязвимостей;
- эффективность существующих или планируемых средств обеспечения информационной безопасности.

Возможность реализации угрозы оценивается вероятностью её реализации в течение заданного отрезка времени для некоторого ресурса АС. При этом вероятность реализации угрозы определяется следующими основными показателями:

- привлекательность ресурса (показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможность использования ресурса для получения дохода (также используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- технические возможности реализации угрозы;
- степень лёгкости реализации уязвимости.

Проведение анализа рисков позволяет:

- предметно описать состав и структуру информационной системы;
- расположить имеющиеся ресурсы по приоритетам, основываясь на степени их важности для полноценного функционирования АС;
- оценить угрозы и идентифицировать уязвимости АС.

Таким образом, было обнаружено некоторое количество актуальных угроз, вот некоторые из нх:

1. Компрометация паролей BIOS или дополнительных аппаратных средств аутентификации;
2. Подбор пароля BIOS (или дополнительных аппаратных средств аутентификации);
3. Использование технологического пароля BIOS;
4. Загрузка сторонней операционной системы (без средств защиты и разграничения доступа к ресурсам компьютера);
5. Предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы;

6. Неумышленное (случайное), преднамеренное копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители, в том числе печать неучтённых копий документов с ПДн на принтерах;

7. Неумышленная (случайная), преднамеренная модификация (искажение) доступных ПДн;

8. Неумышленное (случайное), преднамеренное добавление (фальсификация) ПДн;

9. Неумышленное (случайное), преднамеренное уничтожение доступных ПДн (записей, файлов, форматирование диска, уничтожение носителей);

10. Разглашение (например, при разговорах, записывание на бумаге и т.п.) пользовательских имён и паролей;

11. Использование для входа в систему чужих идентификаторов и паролей;

12. Оставление без присмотра незаблокированных рабочих станций;

13. Внедрение и запуск сторонних программ (технологических, инструментальных и т.п.);

14. Изменение настроек и режимов работы ПО, модификация ПО (удаление, искажение или подмена программных компонентов ИСПДн или СЗИ) (преднамеренное или случайное);

15. Подкючение к ИСПДн стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи);

16. Нарушение работоспособности технических средств;

17. Вмешательство в работу средств защиты (нарушение правил использования);

18. Несанкционированное изменение конфигурационных файлов ПО (настроек экрана, сети, прикладных программ и т.п.);

19. Установка программных "клавиатурных шпионов";

20. Использование нетрадиционных каналов инсайдером для передачи

ПДн;

21. Удаление или искажение регистрационных данных СЗИ (преднамеренное или случайное);

22. Несанкционированный доступ к ПДн на бумажных носителях;

23. Проявление ошибок в программном обеспечении ИСПДн (в том числе в СЗИ);

24. Сбои и отказы технических средств;

25. Использование не учтенных съемных носителей и устройств;

26. Запуск сторонних программ (преднамеренный или не преднамеренный);

27. Программные закладки;

28. Использование программ-анализаторов пакетов (снифферов) для перехвата ПДн (и иной конфиденциальной информации), идентификаторов и паролей удалённого доступа;

29. Выявление активных сетевых служб, используемых портов, версий программ (уязвимых);

30. Выявление не используемых, но установленных сетевых служб (уязвимых);

31. Подбор идентификаторов и паролей пользователей сетевых служб (и их последующее использование).

Для уменьшения риска реализации угроз, были предложены меры противодействия, вот некоторые из них:

1. Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки и защиты информации;

2. Контроль несанкционированного доступа и действий пользователей;

3. Реализация разрешительной системы допуска пользователей;

4. Реализация подсистемы управления доступом; Реализация подсистемы регистрации и учета; Реализация подсистемы надежной идентификации и аутентификации; Реализация подсистемы обеспечения

целостности; Реализация подсистемы антивирусной защиты; Реализация подсистемы централизованного управления СЗПДн;

5. Учет и хранение съемных носителей, и их обращение, исключающее хищение, подмену и уничтожение;

6. Резервирование технических средств, дублирование массивов информации и носителей;

7. Ограничение доступа пользователей в помещения;

8. Предотвращение внедрения в ИС вредоносных программ и программных закладок;

9. Реализация подсистемы безопасного межсетевого взаимодействия; Реализация подсистемы анализа защищенности; Использование защищенных каналов связи; Защита информации криптографическими методами;

10. Размещение технических средств ИСПДн в пределах охраняемой территории.

2.5 Частная модель угроз

Для определения возможных каналов утечки информации, обнаруженных на этапе обследования, необходимо разработать документ Частная модель угроз безопасности ПДн при их обработке в ИСПДн. Этот документ содержит перечень угроз безопасности ИСПДн предприятия, расчет актуальности которых рассчитывался исходя из уровня исходной защищенности, уязвимости, позволяющие осуществить их практическую реализацию, а также методы и способы защиты информации, позволяющие снизить актуальность угроз до приемлемого уровня.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз УБПДн в ИСПДн.

Глава 3. Разработка политики информационной безопасности и организационно-распорядительной документации

3.1 Правовая основа обеспечения ИБ предприятия

Правовой основой обеспечения ИБ являются положения Конституции Российской Федерации, федеральных законов, указов Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, нормативных правовых актов законодательства Российской Федерации, нормативных и руководящих документов ФСТЭК России и ФСБ России по вопросам защиты информации.

Базовыми законами в области обеспечения ИБ является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», устанавливающий необходимость защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Основу правового обеспечения деятельности ФКУ «Налог-Сервис» устанавливает Налоговый кодекс Российской Федерации (НК РФ), вводящий понятие налоговой тайны.

Особое место в правовой основе обеспечения ИБ занимают Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и положения нормативно-методических документов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (КСИИ).

Действующее в настоящее время постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» относит к служебной тайне любую информацию, которая касается деятельности органов государственной власти, ограничение на распространение которой диктуется служебной необходимостью. Должностные лица и работники налоговых органов могут иметь доступ к производственной (коммерческой) тайне налогоплательщиков, поэтому необходимо также руководствоваться

Гражданским кодексом Российской Федерации (ГК РФ) и Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

При организации электронного взаимодействия с другими органами государственной власти, а также оказанием государственных услуг налогоплательщикам, наряду с нормативными документами, регламентирующими технические аспекты защиты телекоммуникационной инфраструктуры системы межведомственного электронного взаимодействия, административными регламентами, необходимо опираться на положения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», обеспечивающего юридическую значимость электронных документов.

3.2 Цели обеспечения безопасности информации на предприятии

Главной целью обеспечения безопасности информации в ФКУ «Налог-Сервис» является предотвращение (минимизация) ущерба субъектам правоотношений в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению (модификации), уничтожению или незаконному использованию, либо нарушению работы ИС налоговых органов и телекоммуникационной инфраструктуры предприятия, используемой для информационного обмена и взаимодействия с органами государственной власти и организациями.

Основными целями обеспечения безопасности информации являются:

– предотвращение несанкционированного доступа к информации;

– предотвращение нарушений прав субъектов при обработке информации;

– предупреждение последствий нарушения порядка доступа к информации;

– недопущение воздействия на технические средства обработки информации;

– недопущение деструктивного информационного воздействия на

информацию.

3.3 Цели и задачи политики информационной безопасности

Политика призвана обеспечить и постоянно поддерживать следующие свойства информации в автоматизированной системе:

– Целостность и аутентичность информации, хранимой, обрабатываемой в АС и передаваемой по информационно-телекоммуникационной сети.

– Конфиденциальность информации ограниченного распространения, хранимой, обрабатываемой СВТ и передаваемой по каналам связи.

– Доступность хранимой и обрабатываемой информации для законных пользователей.

– Предоставить обзор требований к информационной безопасности АС и к отдельным ее компонентам.

– Описание действия над существующими подсистемами и планируемые изменения в них с целью приведения к соответствию указанным требованиям.

– Описать правила поведения и ответственность пользователей, имеющих доступ к системе.

3.4 Порядок внутреннего анализа рисков

Внутренний анализ рисков производится администратором безопасности с привлечением системного администратора с периодичностью не менее одного раза в год.

Целью внутреннего анализа рисков является оценка текущего состояния подсистемы информационной безопасности АС, прогнозирование требуемых затрат на ее поддержание и модернизацию.

Методика проведения внутреннего анализа рисков не регламентируется и

может быть выбрана администратором безопасности в соответствии с организационными особенностями предприятия и параметрами технических средств АС и согласовывается с начальником отдела информационных технологий.

Типовая Модель нарушителя представляется в приложениях к Политике информационной безопасности.

Возможные каналы утечки и Типовая модель угроз информационной безопасности так же представляются в приложениях к Политике информационной безопасности.

Общий анализ рисков проводится в рамках мероприятий по аудиту информационной безопасности в порядке, установленным в Политике информационной безопасности.

3.4.1 Аудит информационной безопасности

Целью аудита информационной безопасности является подтверждение соответствия используемых методов и технологий обеспечения информационной безопасности допустимому уровню риска АС.

Проверки, оценки или подсчёты, связанные с защитой АС, проводятся ответственными сотрудниками под руководством системного администратора и администратора безопасности.

В случае необходимости проведения независимых оценок, соответствия используемых методов и технологий, обеспечения информационной безопасности сторонними организациями, все мероприятия производятся с письменного разрешения (приказа, распоряжения) Руководителя предприятия и под контролем системного администратора. Попытки применения средств анализа защищённости АС, а также попытки нарушения информационной безопасности АС без письменного разрешения Руководителя предприятия не допускаются.

Результаты аудита содержат отчёты по обеспечению безопасности АС в

целом или её логических компонентов. Описания, выявленные факты и рекомендации, полученные в ходе проведения экспертизы, используются для дальнейшей оценки степени риска АС.

Проверки и аудиты могут быть проведены независимо от сотрудников, ответственных за функционирование общей системы поддержки. Необходимые аудиты могут быть осуществлены как изнутри, так и извне АС.

Аудит (комплексная проверка мер по обеспечению информационной безопасности) проводятся не реже одного раза в год. Отдельные проверки систем на потенциальные повреждения осуществляются с периодичностью, необходимой для поддержания требуемого уровня оперативности статистических данных, применяемых для анализа рисков.

3.5 Должностные обязанности администраторов

3.5.1 Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

1. Осуществлять практическую реализацию положений Политики.
2. Осуществлять проектирование, разработку и контроль реализации Политики, а также корректировать ее в соответствии с изменяющейся внутренней и внешней информационной средой.
3. Осуществлять разработку практических требований и рекомендаций по настройке аппаратных, программных и программно-аппаратных средств обеспечения информационной безопасности, применяемых в предприятии.
4. Осуществлять тестирование и экспертизу средств защиты, применяемых в рамках АС.
5. Производить анализ рисков на основе данных аудита.
6. По результатам экспертизы средств защиты предоставлять в распоряжение начальника отдела безопасности отчёт, содержащий план

защиты предприятия, включающий:

– описание уязвимостей, которые могут привести к реализации атак;

– анализ и прогнозирование рисков в соответствии с представленной методикой;

– распределение ролей, обязательств, полномочий и ответственности системных администраторов и пользователей АС;

– документ, описывающий конкретные действия, выполняемые для обнаружения атак в сети предприятия;

– документ, описывающий регулярно выполняемые процедуры проверки и анализа зарегистрированных данных для обнаружения в них следов совершенных атак;

– документ, описывающий процедуры и инструментальные средства взаимосвязи информации об отдельных атаках;

– документ, определяющий потенциальные изменения инфраструктуры, связанные с возможным расширением или реструктуризацией сети по мере ее развития.

7. Другие обязанности администратора информационной безопасности определяются в его должностном регламенте.

3.5.2 Обязанности системного администратора

Системный администратор обязан:

1. Предоставлять администратору информационной безопасности любую информацию относительно параметров, режимов функционирования и особенностей настроек всех информационных систем.

2. Информировать пользователей АС об установленных правилах Политики информационной безопасности и следить за ее выполнением.

3. Обеспечивать практическую реализацию положений Политики информационной безопасности предприятия.

4. Осуществлять распределение ролей, обязательств, полномочий и

ответственности пользователей АС.

5. Следить за выполнением пользователями Политики информационной безопасности.

6. Осуществлять добавление в АС новых пользователей, изменение их полномочий в АС, а также удалять пользователей из АС по указанию администратора информационной безопасности.

7. Обеспечивать работоспособность АС в части технического и системного программного обеспечения.

8. Обеспечивать работоспособность АС антивирусной защиты.

3.6 Планирование мероприятий по информационной безопасности для компонент автоматизированной системы

Для каждого из этапов функционирования компонентов АС предъявляются требования к реализации мер по планированию обеспечения информационной безопасности.

3.6.1 Предпроектная стадия

Предпроектная стадия включает в себя предпроектное исследование вопросов, связанных с предлагаемым компонентом, разработку аналитического обоснования необходимости создания СЗИ и технического задания.

На этом этапе необходимо проанализировать особенности предлагаемого компонента, а также его роль в АС с точки зрения обеспечения информационной безопасности. Необходимо формализовать:

1. назначение компонента;

2. положение компонента в существующей архитектуре АС и предполагаемые изменения архитектуры, связанные с возможным внедрением компонента;

3. уровень конфиденциальности информации, для обработки которой

предназначен компонент;

4. предполагаемое влияние компонента на конфиденциальность, целостность и доступность связанной с ним информации;

5. возможные уязвимости компонента, характерные для области его применения.

3.6.2 Стадия разработки/приобретения

Стадия разработки/приобретения включает в себя комплекс взаимосвязанных организационно-технических мероприятий по созданию, разработки или приобретением компонентов АС. На данной станции необходимо:

1. Руководствоваться формализованными на предпроектной стадии требованиями к обеспечению информационной безопасности.

2. Включить в проектную документацию разделы, содержащие:

- требования к безопасности компонента и ссылки на конкретные архитектурные и технические решения, обеспечивающие их реализацию;
- формально обоснованные процедуры оценки и тестирования компонента на предмет соответствия установленным требованиям к обеспечению информационной безопасности.

3. Предусмотреть возможность обновления защитных мер в случае идентификации новых уязвимостей системы или перехода на новые технологии.

4. В случае если компонент является приобретаемым продуктом или содержит в качестве составляющей объект, являющийся приобретаемым продуктом, необходимо произвести анализ спецификаций и сопутствующей документации этих продуктов на предмет соответствия предъявляемым требованиям.

3.6.3 Стадия установки

Стадия установки включает в себя комплекс взаимосвязанных мероприятий, связанных с внедрением разработанного (приобретенного) компонента в состав АС, а также с осуществлением соответствующих изменений в инфраструктуре АС. На данной стадии необходимо:

1. В процессе установки и настройки системы обеспечить контроль соблюдения требований в области обеспечения информационной безопасности. В частности, в ходе выполнения работ по внедрению компонента не допускается возникновение состояний, при которых АС или её часть становится уязвимой по отношению к внутренним или внешним угрозам конфиденциальности, целостности или доступности информации.
2. Провести комплексное тестирование АС с использованием тестов, включённых в состав проектной документации или спецификации коммерческого продукта.

После окончания внедрения компонента в состав АС необходимо провести внеплановую экспертизу средств защиты.

3.6.4 Стадия функционирования и поддержки

На протяжении данной стадии осуществляется полноценное функционирование внедрённого компонента в составе АС. Необходимо:

1. Строго руководствоваться мерами по обеспечению информационной безопасности компонента, представленными в его технической документации.
2. Проводить периодический контроль эффективности мер защиты информации в отношении данного компонента в рамках плановой или внеплановой экспертизы средств защиты.
3. В случае необходимости вести мониторинг функционирования компонента, а также аудит собранной при этом информации.

3.6.5 Стадия списания

Стадия списания является завершающей в жизненном цикле компонента АС и включает в себя удаление информации, а также уничтожение программного или аппаратного обеспечения. На данной стадии необходимо руководствоваться следующими правилами:

1. В случае возможности дальнейшего использования информации производится её архивирование. При выборе соответствующего носителя архивированной информации необходимо руководствоваться долговечностью носителя, а также распространённостью и документированностью технологии с целью обеспечения беспрепятственного восстановления информации. При хранение информации в зашифрованном виде использованные средства криптографической защиты должны быть сертифицированы.

2. Уничтожение носителей информации должно осуществляться путём физического разрушения, не допускающего последующего восстановления всего носителя или его отдельных частей.

3. В случае принятия решения о дальнейшем использовании носителя (компоненты) информации должно производиться стирание информации посредством программ или технических средств, гарантирующих невозможность последующего восстановления информации.

3.7 Физическая безопасность

Физические меры защиты предназначены для создания физических препятствий на возможных путях проникновения потенциальных нарушителей на территорию предприятия, к компонентам АС и доступа к защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

1. Для разграничения доступа в помещения, где располагается серверное оборудование и другие критически важные объекты АС, целесообразно использовать системы физической защиты, позволяющие регистрировать и контролировать доступ исполнителей и посторонних лиц,

основанные на таких методах идентификации и аутентификации (например: магнитные и электронные карты с личными данными, биометрические характеристики личности пользователей и т.п.).

2. Эксплуатация АРМ и серверов АС должна осуществляться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (АРМ, документов, реквизитов доступа и т.п.).

3. Размещение и установка АРМ и серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения.

4. Уборка помещений, в которых обрабатывается или хранится информация ограниченного доступа и/или служебная информация, должна производиться в присутствии ответственного, за которым закреплено данное помещение или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

5. В помещениях во время обработки и отображения на АРМ информации ограниченного доступа должны находиться только работники, допущенные к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка защищаемой информации.

6. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами. Помещения должны быть обеспечены средствами уничтожения документов.

7. Физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение.

8. Запрещается предоставлять посторонним лицам информацию о том,

что делается в защищенных областях.

9. Для обеспечения должного уровня безопасности и для предотвращения вредоносных действий запрещается работать в одиночку (без надлежащего контроля) с критически важными компонентами АС.

10. В нерабочее время защищенные области должны быть физически недоступны и периодически проверяться охраной.

11. Персоналу, осуществляющему техническое обслуживание сервисов, должен быть предоставлен доступ в защищенные области только в случае необходимости и после получения разрешения.

12. Запрещается использование фотографической, звукозаписывающей и видео аппаратуры в защищенных областях, за исключением санкционированных случаев.

13. По окончании рабочего дня помещения с установленными защищенными АРМ должны сдаваться под охрану с включением сигнализации и с отметкой в книге приема и сдачи служебных помещений.

14. Выносить оборудование, данные и программы за пределы предприятия без установленного документального оформления запрещается.

3.7.1 Защита центров данных и компьютерных залов

Центры данных, серверные комнаты и компьютерные залы, поддерживающие критически важные сервисы организации, должны иметь надежную физическую защиту. При выборе и обустройстве соответствующих помещений необходимо принять во внимание возможность повреждения оборудования в результате пожара, наводнения, взрывов, гражданских беспорядков и других аварий. Следует также рассмотреть угрозы безопасности, которые представляют соседние помещения. Необходимо соблюдать следующие меры:

1. Разместить ключевые системы подальше от общедоступных мест и мест прохождения общественного транспорта.

2. Элементы здания не должны привлекать внимание и выдавать свое назначение (по возможности); не должно быть явных признаков как снаружи, так и внутри здания, указывающих на присутствие вычислительных ресурсов.

3. Внутренние телефонные справочники не должны указывать на местонахождение вычислительных ресурсов.

4. Опасные и горючие материалы следует хранить в соответствии с инструкциями на безопасном расстоянии от месторасположения вычислительных ресурсов.

5. Резервное оборудование и носители информации, на которых хранятся резервные копии, следует разместить на безопасном расстоянии, чтобы избежать их повреждения в случае аварии на основном рабочем месте.

6. Следует установить соответствующее сигнальное и защитное оборудование, например, тепловые и дымовые детекторы, пожарную сигнализацию, средства пожаротушения, а также предусмотреть пожарные лестницы. Сигнальное и защитное оборудование необходимо регулярно проверять в соответствии с инструкциями производителей. Сотрудники должны быть надлежащим образом подготовлены к использованию этого оборудования.

7. Процедуры реагирования на чрезвычайные ситуации должны быть задокументированы, доведены до работников и регулярно тестироваться.

3.7.2 Правила использования рабочего стола

Носители информации, оставленные на рабочих столах, могут быть повреждены или уничтожены в результате аварии, а также могут привести к утечке конфиденциальной информации. В связи с этим предлагаются следующие рекомендации по использованию рабочего стола:

– бумажная документация и съемные носители, когда они не используются, должны храниться в специальных шкафах, особенно в нерабочее время. В случае невозможности хранения и съемных носителей, пользователи

обязаны принять все меры по недопущению посторонних лиц к служебной информации.

– персональные компьютеры и компьютерные терминалы, когда они не используются, необходимо защитить с помощью блокировки с ключом, паролей или других средств контроля.

3.7.3 Источники электропитания

Оборудование необходимо защищать от сбоев в системе электропитании и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования. Следует рассмотреть необходимость использования резервного источника питания. Для оборудования, поддерживающего критически важные производственные сервисы, рекомендуется установить источник бесперебойного питания. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять по окончании срока годности источников бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать в соответствии с рекомендациями изготовителя.

Кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях организации предлагается реализовать следующие защитные меры:

– кабели электропитания и линии связи, идущие к предприятию, должны быть проведены под землей (по возможности) или защищены надлежащим образом с помощью других средств;

– необходимо рассмотреть меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.

3.7.4 Защита оборудования, используемого за пределами предприятия

Использование оборудования информационных систем, поддерживающих производственные процессы, за пределами предприятия должно быть санкционировано руководством. Уровень защиты такого оборудования должен быть таким же, как и для оборудования, расположенного на территории предприятия. Предлагаются следующие рекомендации:

– работникам запрещается использовать персональные компьютеры для продолжения работы на дому;

– во время поездок запрещается оставлять оборудование и носители информации в общедоступных местах без присмотра;

– портативные компьютеры следует провозить в качестве ручного багажа;

– во время поездок портативные компьютеры уязвимы по отношению к кражам, потери и несанкционированного доступа. Для таких компьютеров следует обеспечить надлежащую защиту доступа, чтобы предотвратить несанкционированный доступ к хранящейся в них информации;

– следует всегда соблюдать инструкции производителя, касающиеся защиты оборудования, например, защищать оборудование от воздействия сильных электромагнитных полей.

3.8 Технические средства

3.8.1 Требования к подсистеме идентификации

1. Реализация механизмов идентификации является обязательной для всех подсистем АС должна удовлетворять следующим базовым требованиям:

– уникальность идентификации, в том что каждому пользователю АС должен быть присвоен уникальный идентифицирующий признак, в качестве

которого могут быть использованы:

– уникальная строка символов (логин, или имя пользователя);

– уникальный объект, такой как смарт-карта или жетон.

2. Возможность отслеживания действий пользователя. АС должна иметь возможность идентификации всех активных пользователей, а также протоколирования действий конкретных пользователей в произвольный момент времени.

3. Управление идентификаторами пользователей. Процедуры контроля пользовательских учётных записей должны гарантировать принадлежность всех идентификаторов авторизованным пользователям.

4. Управление неактивными идентификаторами пользователей. В случае не активности пользователя в течение двух месяцев, его учётная запись должна быть заблокирована с возможностью последующего восстановления.

3.8.2 Требования к подсистеме аутентификации.

Реализация механизмов аутентификации является обязательной для всех подсистем АС и должна удовлетворять следующим базовым требованиям:

1. В качестве уникального признака, обеспечивающего реализацию механизмов аутентификации, могут быть использованы:

– секретная информация в виде последовательности символов некоторого конечного алфавита (пароль). (Требования к выбору пароля будут определены позже);

– уникальный, не допускающий копирования предмет (жетон или смарт-карта);

– средства биометрической аутентификации на основании анализа отпечатков пальцев, сетчатки или радужной оболочки глаза, формы кисти руки, а также других уникальных биометрических параметров.

2. Выбор механизма аутентификации и средств, реализующих ту или иную технологию, осуществляется по согласованию с администратором

информационной безопасности и организацией разработчиком информационной АС (подсистемы).

3. Вне зависимости от особенностей применяемой технологии, применяемый уникальный признак ассоциируется с конкретным идентификатором пользователя, который, в свою очередь, принадлежит конкретному лицу (в исключительных случаях - лицам).

3.8.3 Требования к парольной подсистеме.

Парольная подсистема является основой механизмов аутентификации. При использовании паролей в качестве уникальных аутентифицирующих признаков необходимо обеспечить выполнение следующих требований:

1. Минимальная длина пароля составляет 8 символов, максимальная длина не регламентируется и определяется возможностями конкретной среды. В случае необходимости системный администратор может по согласованию с администратором информационной безопасности установить другую фиксированную длину пароля с учётом специфики используемой среды.

2. В числе символов пароля в обязательном порядке должны присутствовать символы минимум из двух следующих алфавитов:

- Латинские прописные буквы:

{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z}

- Латинские строчные буквы:

{a b c d e f g h i j k l m n o p q r s t u v w x y z}

- Арабские цифры:

{0 1 2 3 4 5 6 7 8 9}

- Специальные символы:

{# $ ^ & * _ - + % @},

3. Использование в качестве пароля дат, имён и прочих осмысленных последовательностей символов (в том числе в русской раскладке клавиатуры), не допускается.

4. Пароль не может совпадать с уникальным именем пользователя или с именем пользователя, записанным в обратном порядке.

5. Срок действия пароля устанавливается системным администратором.

6. Изменение пароля пользователя производится пользователем самостоятельно.

7. Изменение паролей уровня администратора сети производится системным администратором.

8. Досрочное изменение пароля производится в следующих случаях:

– в случае дискредитации пароля (т.е. если существует возможность того, что пароль стал известен другому лицу);

– в случае попыток несанкционированного проникновения в АС с использованием уникального имени лица, использующего данный пароль;

– в случае утери (невозможности вспомнить) пользователем пароля;

– в случае прекращения работы пользователя в рамках АС.

9. Системный администратор осуществляет инструктаж пользователей в отношении правил работы с паролями. Акцентируется внимание на недопустимости передачи паролей третьим лицам, а также записи паролей на неучтенный носитель.

10. Пароли пользователей могут храниться в системе исключительно в зашифрованном виде.

11. Возможность просмотра паролей пользователей кем-либо, включая администраторов, не допускается.

12. Во избежание непредвиденных ситуаций, связанных с человеческим фактором, парольная информация учётных записей уровня администратора сети должна быть разделена между сетевым администратором и администратором информационной безопасности.

13. В случае увольнения сотрудника с правами администратора незамедлительно производится досрочная смена всех паролей для пользователей уровня администратора сети.

3.8.4 Требования к системам регистрации сетевых событий

Регистрация сетевых событий представляет собой механизм подотчетности, фиксирующий все события, касающиеся информационной безопасности.

1. Реализация механизма регистрации и аудита сетевых событий преследует следующие цели:

– обеспечение подотчетности пользователей и администраторов;

– обеспечение возможности реконструкции последовательности событий;

– обнаружение попыток нарушений информационной безопасности;

– предоставление исходного материала для последующего анализа эффективности средств защиты.

2. Средства регистрации сетевых событий должны предоставлять следующие возможности:

– ведение и анализ журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для всех средств защиты информации, каждого сервера и всех рабочих станций АС;

– оперативное ознакомление системного администратора с содержимым любого системного журнала;

– получение твёрдой копии журнала регистрации в виде, удобном для последующего анализа;

– упорядочение системных журналов по временным признакам;

– оперативное оповещение администратора информационной безопасности о попытках НСД к ресурсам АС;

– защита информации конфиденциального и служебного характера, содержащейся в системных журналах, от несанкционированного воздействия.

3.9 Функциональные средства

Под функциональными средствами понимаются методы обеспечения безопасности АС, имеющие отношение, прежде всего, к механизмам, выполняемым при непосредственном участии работников предприятия (человеческого фактора).

3.9.1 Работа с персоналом

Меры по организации системы безопасности при работе с АС персоналом призваны минимизировать ущерб, наносимый системе при помощи действий человека, как намеренных, так и не преследующих разрушительных целей. Защита обеспечивается:

1. Неукоснительным соблюдением пользователями правил доступа к АС и выполнение ими своих обязанностей в соответствии с положениями и инструкциями.
2. Реализацией ограничения доступа пользователей к ресурсам АС. При формировании матриц доступа необходимо руководствоваться правилом минимизации полномочий, согласно которому каждый пользователь обеспечивается минимальным количеством ресурсов, необходимых для выполнения функциональных обязанностей.
3. Формированием перечня ресурсов, предоставляемых пользователю, осуществляется на основании занимаемой должности и выполняемых работ. До получения прав доступа пользователь АС должен быть ознакомлен с положениями Политики информационной безопасности и предупреждён об ответственности за невыполнение правил Политики безопасности.
4. Разделением выполнения всех критичных для функционирования АС действий между несколькими лицами. Не допускается возникновение ситуации, когда только один человек имеет права доступа ко всем компонентам АС. В частности, парольная информация учётных записей уровня администратора сети должна быть разделена между системным

администратором и администратором безопасности.

5. Не допускается передача парольной информации пользователями сторонним лицам, а также хранения ее на бумажных или электронных носителях в открытом (незашифрованном) виде.

3.9.2 Планирование непрерывной работы

Мероприятия по планированию непрерывной работы обеспечивают функционирование организации в случае сбоя в информационной поддержке и включают в себя следующие требования:

1. Системный администратор совместно с администратором информационной безопасности разрабатывают инструкции исправления штатных неполадок для всех компонентов сети.

2. Системный администратор совместно с администратором информационной безопасности разрабатывает планы восстановления данных, циркулирующих в АС, обеспечивает возможность продолжения выполнения критических заданий в кратчайшие сроки в случае возникновения непредвиденных ситуаций.

3. Конечные пользователи сети инструктируются системным администратором и администратором информационной безопасности.

Письменные описания действий при возникновении аварийных ситуаций должны быть доступны пользователям.

3.9.3 Средства поддержки программных приложений

Средства поддержки программных приложений призваны обеспечить контроль легальности установленного программного обеспечения при выполнении следующих требований:

1. При введении в эксплуатацию приобретённого или разработанного программного обеспечения необходимо строго следовать определенным ранее

положением.

2. Количество приобретённых лицензий должно соответствовать количеству автоматизированных рабочих мест, на которых установлен программный продукт.

3. Копия легального программного обеспечения, установленная на переносной компьютер (ноутбук), не считается нелегальной и не требует приобретения дополнительных лицензий.

4. Изменения программных приложений или их отдельных компонентов производятся только по согласованию с администратором информационной безопасности.

5. Не допускается использование версий программного обеспечения, не прошедших тестирование.

6. Пользователи системы не имеют права самостоятельно устанавливать, модифицировать или переконфигурировать программное обеспечение без письменного разрешения системного администратора и администратора информационной безопасности.

3.9.4 Средства обеспечения целостности информации

Средства обеспечения целостности информации предназначены для защиты от случайного или преднамеренного изменения, или уничтожения и включают в себя реализацию следующих мер:

1. На каждой рабочей станции должно быть установлено антивирусное программное обеспечение, включающее:

– Антивирусный сканер.

– Резидентный антивирусный монитор.

– Систему антивирусной защиты электронной почты.

– Дисковый ревизор, осуществляющий контроль целостности критических файлов с использованием контрольных сумм.

2. Сигнатуры антивирусных баз должны обновляться ежедневно в

автоматическом или ручном режиме.

3. Должна проводиться регулярная проверка программ и данных в системах, поддерживающих критически важные информационные и технологические процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано.

4. Съемные накопители информации неизвестного происхождения должны проверяться на отсутствие вирусов до их использования.

5. В автоматическом режиме, с целью последующего анализа, должны фиксироваться следующие данные:

– идентификатор пользователя, который последний входил в систему;

– дата и время последнего входа и выхода из системы;

– число неудачных попыток входа в систему.

6. Функции администратора, связанные с назначением прав и полномочий пользователей, не должны быть доступны прочим пользователям и процессам.

7. Контроль целостности конкретных программных и информационных ресурсов должен обеспечиваться как минимум одним из следующих способов:

– Средствами подсчёта и анализа контрольных сумм.

– Средствами электронной цифровой подписи.

– Средствами сравнения критичных ресурсов с их эталонными копиями.

8. Не допускается работа пользователя (в т.ч. администратора) на рабочей станции другого пользователя без разрешения администратора информационной безопасности. Для пользователя, получившего разрешение на работу, не должны быть доступны файлы и каталоги, созданные владельцем рабочей станции. Работа пользователей на рабочих станциях администраторов без контроля с их стороны не допускается.

3.9.5 Документирование

Документирование механизмов безопасности является средством защиты, позволяющим формализовать защитные и функциональные процедуры обеспечения информационной безопасности, характерные для данной системы.

Обязанности должностных лиц в области документирования средств обеспечения информационной безопасности:

1. Администратор информационной безопасности, руководствуясь результатами анализа безопасности сети, составляет документацию.

2. Администратор информационной безопасности обеспечивает автоматическое введение файлов журналов, отражающих все действия пользователя в отношении механизмов обеспечения информационной безопасности.

3. Администратор информационной безопасности на основании данных, предоставленных системным администратором, разрабатывает и модифицирует Политику безопасности, а также рекомендации по реализации конкретных мер защиты сети в виде приложений к Политике безопасности.

3.9.6 Осведомлённость и обучение специалистов

1. Каждый пользователь системы до получения прав доступа к системе должен быть проинструктирован о принятых мерах по обеспечению информационной безопасности.

2. В случае возникновения затруднений в отношении реализации установленных правил, пользователь должен обратиться к системному администратору за помощью.

3. Пользователи, не владеющие установленными правилами, к работе с использованием АС не допускаются.

4. Администратор информационной безопасности и системные администраторы должны обладать уровнем профессиональной подготовки (пройти обучение), достаточным для качественного исполнения

функциональных обязанностей.

3.9.7 Действия в случаях возникновения происшествий

В случае возникновения событий, приводящих к подавлению механизмов обеспечения информационной безопасности или являющихся попыткой преодолеть установленные защитные меры, последовательность ответных действий должна быть следующей:

1. Определение типа происшествия;
2. Локализация источника угрозы;
3. Выработка ответных действий и согласование их с администратором информационной безопасности;
4. Реализация ответных действий;
5. Анализ причины возникновения угрозы и разработка мер по устранению этой причины в последующем.

Каждый из этапов должен сопровождаться документом, описывающим в произвольной форме последовательность предпринятых действий.

Заключение

Процесс широкого внедрения информационных технологий в жизни современных людей вызвал появление ряда общих проблем информационной безопасности:

- необходимость гарантии непрерывности и корректности функционирования основных информационных систем (ИС), главной целью которых является обеспечение безопасности населения и экологической обстановки;

- необходимость обеспечения защиты имущественных прав граждан, предприятий и государства в рамках требований гражданских, административных и хозяйственных прав (в том числе и защита секретов и интеллектуальной собственности);

- необходимость защиты гражданских прав и свобод, которые гарантирует действующее законодательство (в том числе и право на доступ к информации).

В ходе дипломного проектирования были реализованы следующие задачи:

- Проведен анализ информационной системы на рассматриваемой организации;
- Проведен анализ и классификация источников угроз информации;
- Осуществлена разработка частной модели угроз информационной безопасности;
- Осуществлена разработка политики информационной безопасности;
- Осуществлена разработка регламентов, положений и инструкций в области информационной безопасности.

Большинство методов защиты информации от угроз основаны на мероприятиях инженерного и технического рода. Инженерно-технической защитой считаются специальные органы, технические средства и мероприятия, функционирующие с целью совместного выполнения определенных задач по

защите информации.

Инженерно-техническая защита представлена следующими средствами:

- физическими средствами;
- аппаратными средствами;
- программными средствами;
- криптографическими средствами.

К физическим средствам относятся всевозможные инженерные средства и сооружения, целью которых является препятствие физическим проникновениям злоумышленников к объектам защиты и защита персонала (личных средств безопасности), материальных средств и финансов, информации от противоправных действий.

Список используемой литературы

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

3. Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

4. Гражданский кодекс Российской Федерации (ГК РФ);

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

6. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

7. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа»;

8. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

9. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

10. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;

11. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;

12. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;

13. ГОСТ Р ИСО/МЭК 18045 «Методы и средства обеспечения безопасности. Методология оценки безопасности информационных

технологий»;

14. ГОСТ Р ИСО/МЭК 27001-2005 «Информационные технологии. Технологии безопасности. Система управления информационной безопасностью»;

15. Нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный заместителем директора ФСТЭК России 15 февраля 2008 года;

16. Нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный заместителем директора ФСТЭК России 14 февраля 2008 года;

17. Нормативно-методический документ «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденный приказом директора ФСТЭК России от 05 февраля 2010 года №58;

18. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Гостехкомиссия России. 2002 год;

19. Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17 ноября 2007 года №781;

20. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 года №687;

21. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Гостехкомиссия России. 1992 год;

22. Руководящий документ «Средства вычислительной техники.

Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации». Гостехкомиссия России. 1992 год;

23. Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года №188 (с изменениями и дополнениями от 23 сентября 2005 года).