Приложение № 2

к приказу “Об утверждении частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных”

От 18 февраля 2013 г. № 7-1

Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных “Заемщики”

Москва 2013

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией,

поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Распространение персональных данных – распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

СЗИ – средства защиты информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Частная модель угроз безопасности персональных данных (далее – Модель угроз) при их обработке в информационной системе персональных данных “Заемщики” ООО МФО «Саммит» (далее Учреждение), разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.12 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных система персональных данных";
- Приказ ФСТЭК России №21 от 18.02.13 г. “Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);

Модель угроз формируется в соответствии с методическими документами и утверждается генеральным директором Учреждения.

Модель угроз может быть пересмотрена:

1) по решению Учреждения на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

2) по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе;

3) после изменений в составе и территориальном расположении технических средств ИСПДн;

4) по истечению года с момента утверждения настоящей модели угроз или с момента предыдущего пересмотра модели угроз.

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности ПДн и проектирования Системы защиты ИСПДн.

Данная Модель угроз используются при:

1) классификации ИСПДн;

2) разработке Технического задания на создание системы защиты персональных данных, при их обработке в ИСПДн;
3) разработке Плана мероприятий по обеспечению безопасности ПДн;
4) проверке соответствия системы защиты ИСПДн заданным к ней требованиям.

В модели представлено описание структуры ИСПДн, состава и режима обработки ПДн, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

В заключении даны рекомендации по мерам, необходимым для уменьшения опасности актуальных угроз.

1. Описание ИСПДн

1.1 Определение условий создания и использования персональных данных

Характер и структура обрабатываемых персональных данных:

1) цель обработки ПДн в ИСПДн - предоставление займов, в том числе микрозаймов юридическим лицам, индивидуальным предпринимателям и физическим лицам.

2) состав ПДн, обрабатываемых в ИСПДн:

1) Дата рождения;

2) Пол;

3) Средний доход;

4) Ежемесячные платежи в других организациях;

5) Паспортные данные;

6) Фактический адрес проживания;

7) Телефоны;

8) Место работы: адрес, название, фио руководителя, телефон, должность, адрес, телефоны;

9) образование;

10) гражданство;

11) семейное положение;

12) количество членов в семье;

13) количество детей/иждевенцев

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к данным, позволяющим идентифицировать субъекта персональных данных и получить о нем дополнительную информацию.

Объем обрабатываемых персональных данных, превышает 100 000 записей о субъектах персональных данных.

3) Действия осуществляемые с данными в ходе их обработки: сбор, запись, систематизация, накопление, хранение, уточнение, использование, извлечение, предоставление, обезличивание, блокирование, удаление персональных данных;

4) условия прекращения обработки ПДн субъектов – прекращение деятельности юридического лица;

5) субъекты, создающие персональные данные – сотрудники Учреждения, посетители интернет сайта организации;

6) субъекты, которым персональные данные предназначены – сотрудники Учреждения, НБКИ, коллекторские агентства.

7) разграничение доступа к защищаемой информации – разграничение прав доступа реализовано средствами ПО, используемого для обработки ПДн;

8) информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных:

1) АРМ сотрудников,

2) Официальный сайт http://centrzaimov.ru/

3) MS Access (интерфейс) в связке с MSSQL Server

4) Сервер на платформе Windows Server 2008 R2, MSSQL Server 2008

1.2 Описание форм представления персональных данных

Носитель ПДн – материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Основными носителями ПДн в ИСПДн Учреждения являются:

1) видовая информация, представленная в виде текста и изображений различных устройств отображения информации, входящих в состав ИСПДн;

2) информация, обрабатываемая в ИСПДн, представленная в виде байт, IP-протоколов, файлов и других логических структур.

Остальные типы носителей можно исключить по следующим причинам:

1) акустическую (речевую) информацию, так как в ИСПДн не производится голосового ввода персональных данных;

2) информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных сигналов, так как паразитные сигналы ОТСС смешиваются с множеством паразитных сигналов, исходящих от элементов ВТСС и прочих ОТСС.

1.3 Описание структуры ИСПДн

На основе анализа условий создания и использования персональных данных определяются элементы и информация, сопутствующая процессам создания и использования персональных данных.

1.3.1 Дополнительные сведения о программных средствах ИСПДн.

- Используются операционные системы семейства Windows;
- Сервер на платформе Windows Server 2008 R2, MSSQL Server 2008

Установленные средства защиты информации:

- бесплатный антивирус Microsoft Security Essential;

- Linux Proxy Firewall;
- Linux VPN Gate.

Конфигурация элементов ИСПДн.

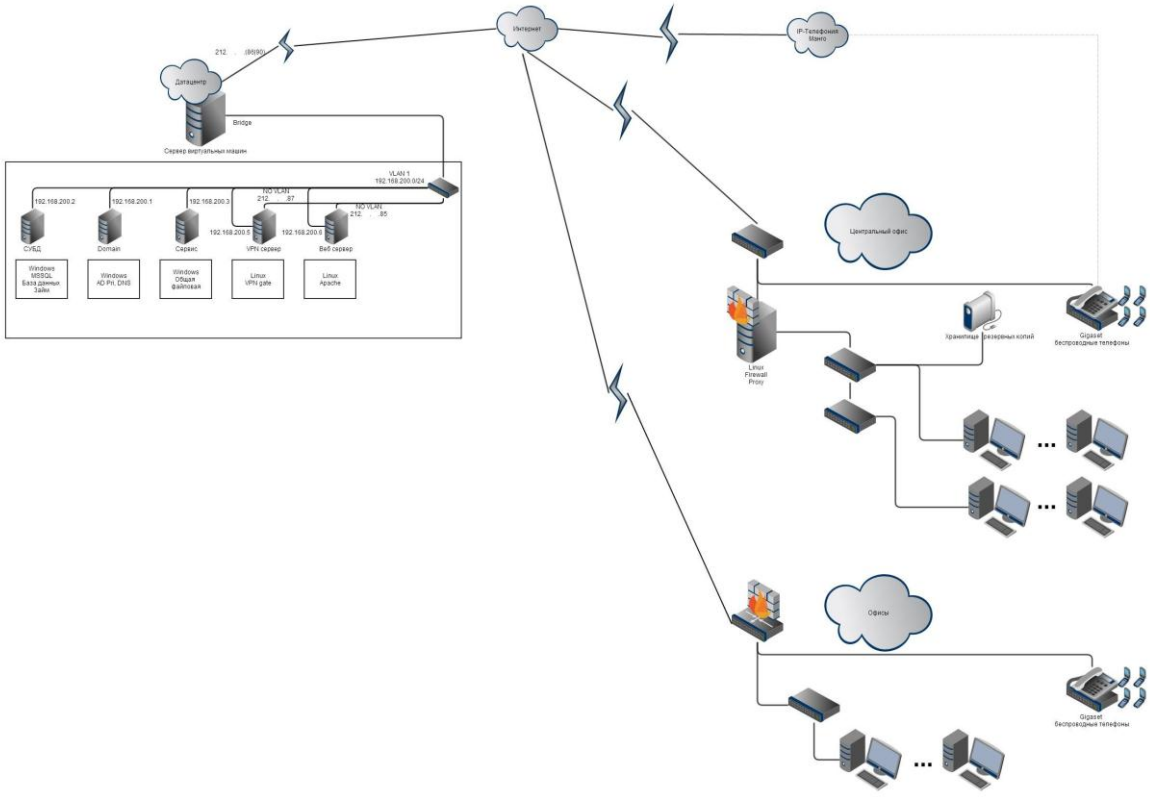

Рисунок 1. Конфигурация элементов ИСПДн

4) Границей контролируемой зоны являются ограждающие конструкции помещений, в которых ведется обработка ПДн.

.

1.4 Определение характеристик безопасности

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

При обработке персональных данных в ИСПДн необходимо обеспечить следующие характеристики безопасности – конфиденциальность, целостность.

Выбранные характеристики безопасности ПДн отражаются в Акте классификации информационной системы персональных данных.

2. Пользователи ИСПДн

В ИСПДн предусмотрены две основные группы пользователей ИСПДн:

1) Администратор БД, имеющий расширенные привилегии в соответствующей подсистеме;

2) Оператор ИСПДн, осуществляющий текущую работу с персональными данными Матрица доступа для ИСПДн Учреждения представлена в таблице 1.

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Администратор БД	Обладает полной информацией о системном и прикладном программном обеспечении соответствующей подсистемы ИСПДн. Обладает частичной информацией о топологии ИСПДн и составе технических средств ИСПДн. Обладает правами конфигурирования и административной настройки программных средств соответствующей подсистемы ИСПДн. Обладает правами доступа к подмножеству ПДн.	Запуск Запись Удаление Чтение Изменение
Оператор ИСПДн	Обладает правами доступа к подмножеству ПДн. Располагает частичной информацией о топологии ИСПДн и составе технических средств ИСПДн. Обладает частичной информа-	Запуск Запись Чтение Изменение

	цией о системном и прикладном программном обеспечении соответствующей подсистемы ИСПДн.	

Таблица 1. Матрица доступа для ИСПДн Учреждения.

Впоследствии сотрудники выявленных групп пользователей, рассматриваются в качестве потенциальных нарушителей.

3. Характеристики ИСПДн

По структуре информационные системы подразделяются:

1) на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

2) на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

3) на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

ИСПДн имеет подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, если вся система или ее элементы пересылают данные по электронным каналам связи в другие системы или имеют подключение к сети Интернет.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

ИСПДн является однопользовательской, когда один сотрудник сочетает в себе роли Администратора и Пользователя ИСПДн, и единолично осуществляет обработку

персональных данных на одном автоматизированном рабочем месте. Во всех других случаях, ИСПДн является многопользовательской.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

ИСПДн является системой с разграничением прав, если в ней присутствуют разные группы пользователей с разными правами. ИСПДн является системой без разграничения прав, когда все пользователи имеют одинаковые права на действия с персональными данными.

Информационные системы **в зависимости от местонахождения** их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Распределенная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляются требования целостности и конфиденциальности

Таблица 2. Параметры ИСПДн.

4. Классификация нарушителей

По наличию права постоянного или разового доступа в КЗ ИСПДн нарушители подразделятся на два типа:

1) внешние нарушители – нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного обмена.

2) внутренние нарушители – нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

4.1 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматриваются физические лица, не имеющие санкционированного постоянного или разового доступа в КЗ.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на получение информации по данному каналу.

В роли внешних нарушителей информационной безопасности могут выступать:

Индекс категории	Категория нарушителя	Описание категории нарушителя
$К_{внешний}1$	Лица не имеющие санкционированного доступа к ИСПДн	— физические лица; — организации (в том числе конкурирующие или террористические); — криминальные группировки.
$К_{внешний}2$	Сотрудники Дата Центра “Караван”	— физические лица, которые могут иметь доступ в помещения, в которых расположено оборудование ИСПДн

4.2 Внутренний нарушитель

Под внутренним нарушителем информационной безопасности рассматривается нарушитель, имеющий непосредственный доступ к каналам связи, техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

К внутренним нарушителям могут относиться:

Индекс категории	Категория нарушителя	Описание категории нарушителя
$К_{вн}1$	Администратор информационной безопасности	Работник, отвечающий за поддержание необходимого уровня безопасности персональных данных в ИСПДн. Назначается приказом руководителя Учреждения
$К_{вн}2$	Пользователи ИСПДн, с повышенными привилегиями	Работники, имеющие повышенные привилегии в соответствующей подсистеме ИСПДн, в т.ч. с правом удаления записей из БД.
$К_{вн}3$	Пользователи ИСПДн	Работники, имеющие санкционированный доступ к ИСПДн
$К_{вн}4$	Работники Учреждения, не имеющие санкционированного доступа к ИСПДн	Работники Учреждения, не имеющие санкционированного доступа к ИСПДн, в т.ч. имеющие санкционированный доступ к общей ЛВС
$К_{вн}5$	Обслуживающий персонал Учреждения	Уборщицы, работники инженерно–технических служб и другие лица, выполняющие обслуживание помещений Учреждения
$К_{вн}6$	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических и программных средств ИСПДн	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн на территории Учреждения
$К_{вн}7$	Администраторы локальной сети	Работники ИТ отдела

Возможности внутреннего нарушителя зависят от действующих в пределах контролируемой зоны защитных мер, основными из которых является реализация системы защиты персональных данных, меры по подбору, обучению и обеспечению лояльности кадров, а так же ограничивающий режим допуска физических лиц внутрь контролируемой зоны.

На лиц категории $К_{вн}1$ возложены задачи по обеспечению безопасности в ИСПДн. Администратор информационной безопасности потенциально может реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации,

обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, исключая средства защиты информации.

Это лицо хорошо знакомо с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что лицо данной категории может использовать стандартное оборудование, либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что это лицо могло бы располагать специализированным оборудованием.

К лицам категории $К_{вн}1$ ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что администратором информационной безопасности будет назначено только доверенное лицо и поэтому будет исключено из числа вероятных нарушителей.

Предполагается, что лица категорий $К_{вн}2$- $К_{вн}7$ относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

4.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:

1) *общая информация* – информации о назначении и общих характеристиках ИСПДн;

2) *эксплуатационная информация* – информация, полученная из эксплуатационной документации;

3) *чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

1) данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

2) сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

3) данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

4) данные о реализованных в СЗИ принципах и алгоритмах;

5) исходные тексты программного обеспечения ИСПДн;

6) сведения о возможных каналах реализации угроз;

7) информацию о способах реализации угроз.

Предполагается, что лица категории $К_{вн}2$ владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИСПДн, использующих эту систему передачи информации. При этом лица категории $К_{вн}2$ не владеют сведениями о возможных каналах реализации угроз, информацией о способах реализации угроз и исходными текстами программного обеспечения ИСПДн.

Предполагается, что лица категории $К_{вн}5$ владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИСПДн, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории $К_{вн}5$ не владеют парольной и аутентифицирующей информацией и по уровню знаний не превосходят категорию $К_{вн}2$.

Предполагается, что лица категории $К_{вн}4$ и лица категории $К_{вн}5$ обладают только общей информацией об ИСПДн.

Предполагается, что лица категории $К_{вн}6$ обладают чувствительной информацией об ИСПДн, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории $К_{вн}6$ к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств.

Таким образом, наиболее информированными об ИСПДн, а следовательно вероятными нарушителями являются лица категории $К_{вн}2$ и $К_{вн}7$.

Степень информированности нарушителя зависит от многих факторов, компетенцию нарушителей, поэтому объективно оценить объем знаний вероятного нарушителя практически невозможно.

В связи с вышеизложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, относится парольная, аутентифицирующая и ключевая информация.

4.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

1) аппаратные компоненты СЗПДн, системы функционирования СЗПДн;

2) доступные в свободной продаже технические средства и программное обеспечение;

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая финансовые возможности и компетенцию нарушителей, поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно, однако считается, что объём обрабатываемой информации не достаточен для применения специальных технических средств.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет доступные в свободной продаже необходимые для реализации угроз средства.

Вместе с тем предполагается, что нарушитель не имеет:

1) средств перехвата в технических каналах утечки;

2) средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

3) средств воздействия на источники и через цепи питания;

4) средств воздействия через цепи заземления;

5) средств активного воздействия на технические средства (средств облучения);

6) дорогостоящих средств для анализа перехваченного трафика.

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории $К_{вн}6$ и $К_{вн}7$.

5. Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн.

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	Средний
2	По наличию соединения с сетями общего пользования	Средний
3	По встроенным (легальным) операциям с записями баз персональных данных	Низкий
4	По разграничению доступа к персональным данным	Средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
6	По уровню (обезличивания) ПДн	Средний
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Средний
8	Исходный уровень защищённости	Средний
9	Значение Y_1	5

Таблица 3. Исходный уровень защищенности.

6. Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

1) **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

2) **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

3) **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

4) **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

6.1 Угрозы утечки информации по техническим каналам

6.1.1 Угрозы утечки акустической (речевой) информации

Описание: Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Внутренний нарушитель:

Обоснование: В ИСПДн Учреждения функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Внешний нарушитель:

Обоснование: В ИСПДн Учреждения функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вывод: Вероятность реализации угрозы – **маловероятно.**

6.1.2 Угрозы утечки видовой информации

Описание: Реализация угрозы утечки видовой информации возможна за счет просмотра информации 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.

Внутренний нарушитель:

Обоснование: В учреждении не принят регламент расположения дисплеев мотитора, относительно посторонних пользователей.

Вывод: Вероятность реализации угрозы – **средняя**.

Внешний нарушитель:

Обоснование: Доступ к дисплеям монитора для сторонних посетителей существенно затруднен.

Вывод: Вероятность реализации угрозы – **низкая**.

6.1.3 Угрозы утечки информации по каналам ПЭМИН

Описание: Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

Внутренний нарушитель:

Обоснование: Паразитный сигнал маскируется с множеством других паразитных сигналов элементов, не входящих в состав ИСПДн. Исходя из предположений об имеющихся у нарушителей технических средствах перехвата информации, внутренние нарушители не могут иметь необходимых для перехвата ПЭМИН технических средств.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Внешний нарушитель:

Обоснование: Паразитный сигнал маскируется с множеством других паразитных сигналов элементов, не входящих в состав ИСПДн. Исходя из предположений об имеющихся у нарушителей технических средствах перехвата информации, внешние нарушители не могут иметь необходимых для перехвата ПЭМИН технических средств.

Вывод: Вероятность реализации угрозы – **маловероятно.**

6.2 Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

1) нарушению конфиденциальности (копирование, неправомерное распространение);
2) нарушению целостности (уничтожение, изменение);

6.2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

Кража ПЭВМ.

Описание: Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Внутренний нарушитель:

Обоснование: Кража ПЭВМ внутренними нарушителями исключается принятыми организационными мерами. Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Внешний нарушитель:

Обоснование: Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Кража носителей информации

Описание: Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

Внутренний нарушитель:

Обоснование: Все носители информации, содержащие выгруженную из ИСПДн информацию, хранятся в запираемых шкафах или сейфах.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Внешний нарушитель:

Обоснование: Двери, при отсутствии сотрудников в помещении, закрываются на замок. Все носители информации, содержащие выгруженную из ИСПДн информацию, хранятся в запираемых шкафах или сейфах.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Кража ключей и атрибутов доступа

Описание: Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

Обоснование: В учреждении не используются ключи и материальные атрибуты доступа.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Внешний нарушитель:

Обоснование: В учреждении не используются ключи и материальные атрибуты доступа.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Кражи, модификации, уничтожения информации

Описание: Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

Внутренний нарушитель:

Обоснование: Доступ к ИСПДн осуществляется согласно утвержденному перечню должностей. Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **средняя.**

Внешний нарушитель:

Обоснование: Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Несанкционированное отключение средств защиты

Описание: Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

Внутренний нарушитель:

Обоснование: В учреждении не принято мер по предотвращению данной угрозы внутренними нарушителями.

Вывод: Вероятность реализации угрозы – **высокая.**

Внешний нарушитель:

Обоснование: Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **маловероятно.**

6.2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

Действия вредоносных программ (вирусов).

Описание: Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

1) скрывать признаки своего присутствия в программной среде компьютера;

2) обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

3) разрушать (искажать произвольным образом) код программ в оперативной памяти;

4) выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

5) сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

6) искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Обоснование: Возможность реализации данной угрозы уменьшается установленными антивирусными средствами, не проходившими в установленном порядке процедуру оценки соответствия.

Вывод: Вероятность реализации угрозы – **средняя.**

Недекларированные возможности системного ПО и ПО для обработки персональных данных.

Описание: Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Обоснование: Установленное в Учреждении системное ПО и ПО для обработки ПДн произведено доверенными разработчиками ПО.

Вывод: Вероятность реализации угрозы – **маловероятно**.

Установка ПО не связанного с исполнением служебных обязанностей

Описание: Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Обоснование: В учреждении не принято мер по противодействию данному виду угроз.

Вывод: Вероятность реализации угрозы – **высокая**.

6.2.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в

программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Утрата ключей и атрибутов доступа

Описание: Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Обоснование: В учреждении не принята парольная политика.

Вывод: Вероятность реализации угрозы – **высокая**.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Описание: Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

Обоснование: В учреждении производится резервное копирование ключевых БД, содержащих ПДн.

Вывод: Вероятность реализации угрозы – **средняя**.

Непреднамеренное отключение средств защиты

Описание: Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

Обоснование: В учреждении не принято мер по противодействию данному виду угроз.

Вывод: Вероятность реализации угрозы – **высокая**.

Выход из строя аппаратно-программных средств

Описание: Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

Обоснование: Сервер установлен на технической площадке дата центра, на размещение сервера имеется подписанный договор.

Вывод: Вероятность реализации угрозы – **средняя.**

Сбой системы электроснабжения

Описание: Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности защищаемой информации.

Обоснование: В учреждении к ключевым АРМ, входящих в состав ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – **маловероятно.**

Стихийное бедствие

Описание: Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

Обоснование: Во всех защищаемых помещениях учреждения установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вывод: Вероятность реализации угрозы – **маловероятно.**

6.2.4 Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

Описание: Угроза осуществляется путем НСД внутренних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

Обоснование: Двери, при отсутствии сотрудников в помещении, закрываются на замок.

Вывод: Вероятность реализации угрозы – **средняя.**

Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

Описание: Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

Обоснование: В учреждении подписаны документы о сохранении коммерческой тайны учреждения.

Вывод: Вероятность реализации угрозы – **низкая**.

Модификация базовой системы ввода/вывода(BIOS), перехват управления загрузкой

Описание: Угроза реализуется внутренними нарушителями путем НСД к защищаемым АРМ. Используемые нарушителем уязвимости: отсутствие пароля на изменение настроек BIOS, отсутствие контроля за подключением отчуждаемых носителей информации.

Обоснование: В учреждении не принято мер по противодействию данному виду угроз.

Вывод: Вероятность реализации угрозы – **высокая**.

6.2.5 Угрозы несанкционированного доступа по каналам связи

В соответствии со структурой информационной системы и определенным характеристикам безопасности, для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

1) угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн информации;

2) угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

3) угрозы выявления паролей по сети;

4) угрозы подмены доверенного объекта в сети;

5) угрозы удаленного запуска приложений;

6) угрозы внедрения по сети вредоносных программ;

Угроза «Анализ сетевого трафика»

Описание: Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

1) изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами,

в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

2) перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Обоснование: Поскольку передача персональных данных по сети “Интернет” осуществляется не чаще 1 раза в месяц, внешний нарушитель не может иметь мотивации для реализации данного вида атак.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Угроза «сканирование сети»

Описание: Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Обоснование: Поскольку сервер с базой данных защищен от воздействия из глобальной сети межсетевым экраном, а так же на нем отсутствует глобальный интерфейс, вероятность реализации данного типа угроз существенно снижается.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Угроза выявления паролей

Описание: Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Обоснование: Поскольку сервер с базой данных защищен от воздействия из глобальной сети межсетевым экраном, а так же на нем отсутствует глобальный интерфейс, вероятность реализации данного типа угроз существенно снижается.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Угрозы подмены доверенного объекта

Описание: Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

Реализация угрозы внутри ЛВС учреждения:

Обоснование: Поскольку взаимодействие между сервером БД и удаленными АРМ осуществляется посредством VPN, вероятность реализации данного вида атак существенно снижается.

Вывод: Вероятность реализации угрозы – **маловероятно.**

Угрозы удаленного запуска приложений

Описание: Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, до-

ступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

1) распространение файлов, содержащих несанкционированный исполняемый код;

2) удаленный запуск приложения путем переполнения буфера приложений-серверов;

3) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Обоснование: В учреждении не принято мер по противодействию данному виду угроз.

Вывод: Вероятность реализации угрозы – **высокая.**

Угрозы внедрения по сети вредоносных программ

Описание: К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является

возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

1) программы подбора и вскрытия паролей;

2) программы, реализующие угрозы;

3) программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

4) программы-генераторы компьютерных вирусов;

5) программы, демонстрирующие уязвимости средств защиты информации и др.

Обоснование: Возможность реализации данной угрозы уменьшается установленными антивирусными средствами, не проходившими в установленном порядке процедуру оценки соответствия.

Вывод: Вероятность реализации угрозы – **средняя.**

7. Реализуемость угроз

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 $Y = (Y_1 + Y_2)/20$

Оценка реализуемости УБПДн представлена в таблице.

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации		
1.1.1. Утечки акустической информации, реализуемые внутренними нарушителями	0,25	низкая
1.1.2. Утечки акустической информации, реализуемые внешними нарушителями	0,25	низкая
1.2. Угрозы утечки видовой информации		

1.2.1. Утечки видовой информации, реализуемые внутренними нарушителями	0,5	средняя
1.2.2. Утечки видовой информации, реализуемые внешними нарушителями	0,35	средняя
1.3. Угрозы утечки информации по каналам ПЭМИН		
1.3.1. Утечки информации по каналам ПЭМИН, реализуемые внутренними нарушителями	0,25	низкая
1.3.2. Утечки информации по каналам ПЭМИН, реализуемые внешними нарушителями	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ		
2.1.1.1. Кража ПЭВМ, осуществляемая внутренними нарушителями	0,25	низкая
2.1.1.2. Кража ПЭВМ, осуществляемая внешними нарушителями	0,25	низкая
2.1.2. Кража носителей информации		
2.1.2.1. Кража носителей информации, осуществляемая внутренними нарушителями	0,25	низкая
2.1.2.2. Кража носителей информации, осуществляемая внешними нарушителями	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа		
2.1.3.1. Кража ключей и атрибутов доступа, осуществляемая внутренними нарушителями	0,25	низкая
2.1.3.2. Кража ключей и атрибутов доступа, осуществляемая внешними нарушителями	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации		
2.1.4.1. Кража, модификация, уничтожение информации, осуществляемые внутренними нарушителями	0,5	средняя
2.1.4.2. Кража, модификация, уничтожение ин-	0,25	низкая

формации, осуществляемые внешними нарушителями		
2.1.5. Несанкционированное отключение средств защиты		
2.1.5.1. Несанкционированное отключение средств защиты, осуществляемое внутренними нарушителями	0,75	высокая
2.1.5.2. Несанкционированное отключение средств защиты, осуществляемое внешними нарушителями	0,25	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,5	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,75	высокая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа	0,75	высокая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,5	средняя
2.3.3. Непреднамеренное отключение средств защиты	0,75	высокая
2.3.4. Выход из строя аппаратно-программных средств	0,5	средняя
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уни-	0,5	средняя

чтожение лицами, не допущенными к ее обработке		
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,35	средняя
2.4.3. Модификация базовой системы ввода/вывода (BIOS), перехват управления загрузкой	0,75	высокая
2.5.Угрозы несанкционированного доступа по каналам связи		
2.5.1. Анализ сетевого трафика	0,25	низкая
2.5.2. Угрозы сканирования сети	0,25	низкая
2.5.3. Угрозы выявления паролей по сети	0,25	низкая
2.5.4. Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.5. Угрозы удаленного запуска приложений	0,75	высокая
2.5.6.Угрозы внедрения по сети вредоносных программ	0,5	средняя

Таблица 4. Реализуемость УБПДн.

8. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

1) **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

2) **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

3) **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая

1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	средняя
2.1.2. Кража носителей информации	средняя
2.1.3. Кража ключей и атрибутов доступа	низкая
2.1.4. Кража, модификация, уничтожение информации	средняя
2.1.5. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	средняя
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лицами,	средняя

не допущенными к ее обработке	
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	средняя
2.4.3. Модификация базовой системы ввода/вывода(BIOS), перехват управления загрузкой	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика»	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	низкая
2.5.4.Угрозы подмены доверенного объекта в сети	средняя
2.5.5.Угрозы удаленного запуска приложений	средняя
2.5.6.Угрозы внедрения по сети вредоносных программ	средняя

Таблица 5. Опасность УБПДн.

9. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Возможность реализации	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Таблица 6. Правила определения актуальности УБПДн.

Оценка актуальности угроз безопасности представлена в таблице.

Тип угроз безопасности ПДн	Актуальность угрозы
1.1. Угрозы утечки акустической информации	
1.1.1. Утечки акустической информации, реализуемые внутренними нарушителями	неактуальная
1.1.2. Утечки акустической информации, реализуемые внешними нарушителями	неактуальная
1.2. Угрозы утечки видовой информации	
1.2.1. Утечки видовой информации, реализуемые внутренними нарушителями	неактуальная
1.2.2. Утечки видовой информации, реализуемые внешними нарушителями	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	
1.3.1. Утечки информации по каналам ПЭМИН, реализуемые внутренними нарушителями	неактуальная
1.3.2. Утечки информации по каналам ПЭМИН, реализуемые внешними нарушителями	неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	
2.1.1.1. Кража ПЭВМ, осуществляемая внутренними нарушителями	неактуальная
2.1.1.2. Кража ПЭВМ, осуществляемая внешними нарушителями	неактуальная
2.1.2. Кража носителей информации	
2.1.2.1. Кража носителей информации, осуществляемая внутренними нарушителями	неактуальная
2.1.2.2. Кража носителей информации, осуществляемая внешними нарушителями	неактуальная
2.1.3. Кража ключей и атрибутов доступа	
2.1.3.1. Кража ключей и атрибутов доступа, осуществляемая внутренними нарушителями	неактуальная
2.1.3.2. Кража ключей и атрибутов доступа, осуществляемая	неактуальная

внешними нарушителями	
2.1.4. Кражи, модификации, уничтожения информации	
2.1.4.1. Кража, модификация, уничтожение информации, осуществляемые внутренними нарушителями	актуальная
2.1.4.2. Кража, модификация, уничтожение информации, осуществляемые внешними нарушителями	неактуальная
2.1.5. Несанкционированное отключение средств защиты	
2.1.5.1. Несанкционированное отключение средств защиты, осуществляемое внутренними нарушителями	актуальная
2.1.5.2. Несанкционированное отключение средств защиты, осуществляемое внешними нарушителями	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	актуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная
2.3.3. Непреднамеренное отключение средств защиты	актуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	

2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	актуальная
2.4.3. Модификация базовой системы ввода/вывода(BIOS), перехват управления загрузкой	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1. Анализ сетевого трафика	неактуальная
2.5.2.Угрозы сканирования сети	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4. Угрозы подмены доверенного объекта в сети	неактуальная
2.5.5. Угрозы удаленного запуска приложений	актуальная
2.5.6.Угрозы внедрения по сети вредоносных программ	актуальная

Таблица 7. Актуальность УБПДн.

Были выявлены следующие актуальные угрозы:

1. Кража, модификация, уничтожение информации, осуществляемые внутренними нарушителями
2. Несанкционированное отключение средств защиты, осуществляемое внутренними нарушителями
3. Действия вредоносных программ (вирусов)
4. Установка ПО, не связанного с исполнением служебных обязанностей
5. Утрата ключей и атрибутов доступа
6. Непреднамеренная модификация (уничтожение) информации сотрудниками
7. Непреднамеренное отключение средств защиты
8. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке
9. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
10. Модификация базовой системы ввода/вывода (BIOS), пе-

рехват управления загрузкой

11. Угрозы удаленного запуска приложений
12. Угрозы внедрения по сети вредоносных программ

10. Меры по противодействию актуальным угрозам безопасности

Наименование угрозы	Меры по противодействию угрозе	
	Технические	Организационные
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.4. Угрозы кражи, модификации, уничтожения информации.		
2.1.4.1. Кража, модификация, уничтожение информации, осуществляемые внутренними нарушителями	Система защиты от НСД	Издание локальных актов, устанавливающих политику учреждения в области обработки и защиты персональных данных и ознакомление с ними сотрудников
2.1.5.1. Несанкционированное отключение средств защиты, осуществляемое внутренними нарушителями	Паролирование изменения настроек СЗИ	
	Настройка сертифицированных СЗИ от НСД	
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);		
2.2.1. Действия вредоносных программ (вирусов)	Установка сертифицированного антивирусного ПО	Инструкция пользователя
		Инструкция администратора информационной безопасности
2.2.3. Установка ПО, не связанного с исполнени-	Настройка средств защиты	Инструкция пользователя

ем служебных обязанностей	Ведение политики администрирования защищаемых АРМ	Инструкция администратора информационной безопасности
	Удаление всех программ, не связанных с исполнением служебных обязанностей	
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа		Инструкция пользователя
		Инструкция администратора информационной безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками		Инструкция пользователя
2.3.3. Непреднамеренное отключение средств защиты	Паролирование изменения настроек СЗИ	Инструкция пользователя ИСПДн
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Система защиты от НСД	Инструкция пользователя
2.4.2. Разглашение информации, модификация,		Проведение первичного инструктажа по реа-

уничтожение сотрудниками допущенными к ее обработке		лизации режима безопасности ПДн
	DLP системы	Инструкция пользователя
		Соглашение о не разглашении
2.4.3. Модификация базовой системы ввода/вывода(BIOS), перехват управления загрузкой	Паролирование настроек BIOS	Опечатывание системных блоков защищаемых АРМ
	Средства доверенной загрузки	
2.5. Угрозы несанкционированного доступа по каналам связи		
2.5.7. Угрозы удаленного запуска приложений	Сертифицированный межсетевой экран	Инструкция администратора информационной безопасности
	HIPS	Инструкция пользователя
2.5.8. Угрозы внедрения по сети вредоносных программ	Сертифицированный межсетевой экран	Инструкция администратора информационной безопасности
	Сертифицированное антивирусное средство	

Таблица 8. Угрозы безопасности и возможные меры по противодействия им.

С учетом специфики учреждения, для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

1) Установить сертифицированные СЗИ от НСД, в том числе, реализующие контроль целостности защищаемых информационных ресурсов, установить пароли на изменение настроек СЗИ.

2) Установить антивирусные средства с сертифицированного дистрибутива и настроить их обновление.

3) Администратору информационной безопасности установить пароли на изменение настроек BIOS на всех защищаемых АРМ.

4) Опечатать системные блоки защищаемых АРМ.

5) Установить и настроить сертифицированные межсетевые экраны.

6) Администратору информационной безопасности сформировать политику администрирования защищаемых АРМ, с учетом настоящей модели угроз и установленных СЗИ от НСД.

7) Удалить все программы, не связанные с исполнением служебных обязанностей.

8) Провести первичный инструктаж по реализации режима безопасности ПДн.

9) Издать локальные акты, устанавливающие политику учреждения в области обработки и защиты персональных данных и ознакомить с ними сотрудников под роспись.

10) Издать инструкцию пользователя, инструкцию администратора информационной безопасности, ознакомить соответствующих сотрудников с ними под роспись.