|  |
| --- |
| Утверждаю  руководитель  «Наименование учреждения»  \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

**Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных «Наименование учреждения»**

20\_\_\_

ОГЛАВЛЕНИЕ

[Определения 2](#_Toc389475509)

[Обозначения и сокращения 2](#_Toc389475510)

[Введение 2](#_Toc389475511)

[Вероятность реализации УБПДн 2](#_Toc389475512)

[Исходный уровень защищенности ИСПДн 2](#_Toc389475513)

[Реализуемость угроз 2](#_Toc389475514)

[Оценка опасности угроз 2](#_Toc389475515)

[Модель нарушителя безопасности персональных данных 2](#_Toc389475516)

[Описание нарушителей 2](#_Toc389475517)

[Предположения о возможностях нарушителя 2](#_Toc389475518)

[Предположения об имеющихся у нарушителя средствах атак 2](#_Toc389475519)

[Описание каналов атак 2](#_Toc389475520)

[Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации 2](#_Toc389475521)

[ИСПДн «Наименование системы» 2](#_Toc389475522)

[Исходный уровень защищенности ИСПДн 2](#_Toc389475523)

[Вероятность реализации УБПДн 2](#_Toc389475524)

[Угрозы утечки информации по техническим каналам 2](#_Toc389475525)

[Угрозы несанкционированного доступа к информации 2](#_Toc389475526)

[Реализуемость угроз 2](#_Toc389475527)

[Оценка опасности угроз 2](#_Toc389475528)

[Определение актуальности угроз в ИСПДн 2](#_Toc389475529)

# 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.

Аутентификация отправителя данных – подтверждение того, что от­правитель полученных данных соответствует заявленному.

**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.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами не­санкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но со­храняют способность к дальнейшему распространению и самовоспроизведе­нию.

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

**Вспомогательные технические средства и системы** – технические сред­ства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средст­вами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персо­нальных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных про­грамм.

Доступ к информации – возможность получения информации и ее ис­пользования.

Закладочное устройство – элемент средства съема информации, скрыт­но внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, пред­меты интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хра­нения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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.

Конфиденциальность персональных данных – обязательное для соблю­дения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных дан­ных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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 невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональ­ными данными, включая сбор, систематизацию, накопление, хранение, уточ­нение (обновление, изменение), использование, распространение (в том чис­ле передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор** (персональных данных) – государственный орган, муниципальный орган, юридиче­ское или физическое лицо, организующее и (или) осуществляющее обработ­ку персональных данных, а также определяющее цели и содержание обра­ботки персональных данных.

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.

**Перехват (информации)** – неправомерное получение информации с ис­пользованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к определен­ному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущест­венное положение, образование, профессия, доходы, другая информация.

**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.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**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.

**Программное (программно-математическое) воздействие** – несанкцио­нированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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.

Утечка (защищаемой) информации по техническим каналам – некон­тролируемое распространение информации от носителя защищаемой инфор­мации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

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

АВС – антивирусные средства

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

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

# Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн «Наименование учреждения» (далее - Учреждение) строится на основании [внутренней проверки](file:///D:\ЗИ\Другие%20МИАЦ\Ханты-Мансийский%20АО\Приложения\Приложение%208%20Отчет%20о%20результатах%20проведения%20внутренней%20проверки.doc).

В модели угроз представлена оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

* Описание угроз.
* Оценку вероятности возникновения угроз.
* Оценку реализуемости угроз.
* Оценку опасности угроз.
* Определение актуальности угроз.

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

## 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 (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

* **маловероятно -** отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
* **низкая вероятность**- объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
* **средняя вероятность** *-* объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
* **высокая вероятность** *-* объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

## Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

#### Угрозы утечки акустической (речевой) информации

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.

#### Угрозы утечки видовой информации

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.

#### Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за нали­чия паразитных электромагнитных излучений у элементов ИСПДн.

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

##### Кража ПЭВМ

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

##### Кража носителей информации

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

##### Кража ключей и атрибутов доступа

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

##### Кражи, модификации, уничтожения информации

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

##### Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

##### Несанкционированное отключение средств защиты

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

#### 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).

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:

* скрывать признаки своего присутствия в программной среде компью­тера;
* обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
* разрушать (искажать произвольным образом) код программ в опера­тивной памяти;
* выполнять без инициирования со стороны пользователя (пользователь­ской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
* сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
* 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.

##### Недекларированные возможности системного ПО и ПО для обработки персональных данных.

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.

##### Установка ПО не связанного с исполнением служебных обязанностей

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

#### 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.

##### Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике 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.

##### Непреднамеренная модификация (уничтожение) информации сотрудниками

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

##### Непреднамеренное отключение средств защиты

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.

##### Выход из строя аппаратно-программных средств

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

##### Сбой системы электроснабжения

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

##### Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

#### Угрозы преднамеренных действий внутренних нарушителей

##### Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

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

##### Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

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

#### Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

* угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
* 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.;
* угрозы выявления паролей по сети;
* угрозы навязывание ложного маршрута сети;
* угрозы подмены доверенного объекта в сети;
* угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
* угрозы типа «Отказ в обслуживании»;
* угрозы удаленного запуска приложений;
* угрозы внедрения по сети вредоносных программ.

##### Угроза «Анализ сетевого трафика»

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:

* 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;
* 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.

##### Угроза «сканирование сети»

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.

##### Угроза выявления паролей

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.

##### Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисег­ментного или межсегментного навязывания. Возможность навязывания лож­ного маршрута обусловлена недостатками, присущими алгоритмам маршру­тизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкцио­нированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени се­тевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

##### Угрозы подмены доверенного объекта

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.

##### Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов уда­ленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом су­ществует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому из­менению маршрутно-адресных данных. В дальнейшем весь поток информа­ции, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

##### Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспече­ния, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступаю­щие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресур­сов ИСПДн на обработку пакетов, передаваемых злоумышленником со сни­жением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Приме­рами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установ­ление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
* явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы че­рез сеть из-за недоступности среды передачи, либо получают отказ в обслу­живании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широко­вещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
* явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушите­лем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
* явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую макси­мально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение рабо­тоспособности соответствующей службы предоставления удаленного досту­па к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

##### Угрозы удаленного запуска приложений

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

* распространение файлов, содержащих несанкционированный исполняемый код;
* удаленный запуск приложения путем переполнения буфера приложений-серверов;
* 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.

##### Угрозы внедрения по сети вредоносных программ

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:

* программы подбора и вскрытия паролей;
* программы, реализующие угрозы;
* программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
* программы-генераторы компьютерных вирусов;
* программы, демонстрирующие уязвимости средств защиты информа­ции и др.

## Реализуемость угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

## Оценка опасности угроз

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

* низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
* средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
* высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.
* В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.
* Таблица 1 – Правила определения актуальности УБПДн

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

# Модель нарушителя безопасности персональных данных

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;
2. Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;
3. СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

## *Описание нарушителей*

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

* + категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;
  + категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

* + внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;
  + внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

* + бывшие сотрудники предприятий отрасли;
  + посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
  + представители преступных организаций. Внешний нарушитель может осуществлять:
  + перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
  + деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
  + несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
  + перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;
  + атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К **первой группе** относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

* + располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;
  + изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

1. Ко **второй группе** относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

* + обладает всеми возможностями лиц первой категории;
  + знает, по меньшей мере, одно легальное имя доступа;
  + обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
  + располагает ПДн, к которым имеет доступ.

1. К **третьей группе** относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной или распределенной сети предприятий.

Лицо данной группы:

* + обладает всеми возможностями лиц второй категории;
  + располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
  + имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

1. К **четвертой группе** относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо данной группы:

* + Обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн
  + Обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
  + имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
  + имеет доступ ко всем техническим средствам сегмента ИСПДн;
  + обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

1. К **пятой группе** относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа.

Лицо данной группы:

* + Обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
  + обладает полной информацией о ТС и конфигурации ИСПДн
  + имеет доступ ко всем ТС ИСПДн и данным;
  + обладает правами конфигурирования и административной настройки ТС ИСПДн.

1. К **шестой группе** относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

* + обладает полной информацией об ИСПДн;
  + имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
  + не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

1. К **седьмой группе** относятся лица из числа программистов- разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

* + Обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
  + обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;
  + может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

1. К **восьмой группе** относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

* + обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
  + может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

## 

## *Предположения о возможностях нарушителя*

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

В дополнении к приведенным в подразделе 9.2 возможностям, которыми обладают различные группы внутренних нарушителей, может быть приведен ряд дополнительных возможностей, которые присущи всем группам внутреннего нарушителя.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

* + предотвращение и пресечение несанкционированных действий;
  + подбор и расстановку кадров;
  + допуск физических лиц в контролируемую зону и к средства вычислительной техники;
  + контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

## *Предположения об имеющихся у нарушителя средствах атак*

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

* + доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
  + специально разработанные технические средства и программное обеспечение;
  + средства перехвата и анализа информационных потоков в каналах связи;
  + специальные технические средства перехвата информации по ТКУИ; штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

## *Описание каналов атак*

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

* + каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
  + электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
  + бумажные носители информации;
  + штатные программно-аппаратные средства ИСПДн;
  + кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
  + незащищенные каналы связи;
  + ТКУИ.

## *Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации*

При взаимодействии отдельных подсистем ИСПДн между собой по сетям связи общего пользования и (или) сетям международного информационного обмена, при обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами, а также при передаче ПДн по кабельным системам, расположенным в пределах контролируемой зоны и не защищенных от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности и целостности информации необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей 9.1.

Таблица 9.1 – Соответствие типов нарушителя и класса СКЗИ

|  |  |  |
| --- | --- | --- |
| **Группа внутреннего нарушителя** | **Тип нарушителя** | **Класс СКЗИ** |
| Группа 1 | Н2 | КС2 |
| Группа 2 | Н3 | КС3 |
| Группа 3 | Н3 | КС3 |
| Группа 4 | Н3 | КС3 |
| Группа 5 | Н3 | КС3 |
| Группа 6 | Н3 | КС3 |
| Группа 7 | Н5 | КВ2 |
| Группа 8 | Н4 | КВ1 |

Внешний нарушитель относится к типу Н1. При этом, если он обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа Нi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Нi (2 <= i <= 6).

Предполагается также, что возможности нарушителя типа Нi+1 включают в себя возможности нарушителя типа Нi (1 <= i <= 5).

# ИСПДн «Наименование системы»

## Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн «Система».

Таблица 2 – Исходный уровень защищенности

|  |  |  |
| --- | --- | --- |
| **Позиция** | **Технические и эксплуатационные характеристики** | **Уровень защищенности** |
| 1 | По территориальному размещению | низкий |
| 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 | низкий |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | низкий |

(Уровни защищенности проставляем согласно методики, стр. 21-22)

Исходный уровень защищенности ИСПДн **низкий (Y1=10)**.

## Вероятность реализации УБПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

### Угрозы утечки информации по техническим каналам

#### Угрозы утечки видовой информации

В учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

#### Угрозы утечки информации по каналам ПЭМИН

Угрозы данного класса имеют **среднюю вероятность**, т.к. размер контролируемой зоны небольшой, но элементы ИСПД находятся в самом центре здания и экранируются блочным перекрытием, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн. **Необходимость применения средств защиты информации должно быть исследовано дополнительно (Y2=5)**.

### 

### Угрозы несанкционированного доступа к информации

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

##### Кража ПЭВМ

В учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятной (Y2=0)**.

##### Кража носителей информации

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Кража ключей и атрибутов доступа

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, организовано хранение ключей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Кражи, модификации, уничтожения информации

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Вывод из строя узлов ПЭВМ, каналов связи

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Несанкционированное отключение средств защиты

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – **низкая (Y2=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).

В Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая (Y2=2)**.

##### Недекларированные возможности системного ПО и ПО для обработки персональных данных.

В Учреждении нет программного обеспечения, разработанного собственными разработчиками специалистами.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Установка ПО, не связанного с исполнением служебных обязанностей

В Учреждении введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы – **низкая (Y2=2)**.

#### 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.

##### Утрата ключей и атрибутов доступа

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **низкая (Y2=2)**.

##### Непреднамеренная модификация (уничтожение) информации сотрудниками

В Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Непреднамеренное отключение средств защиты

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **низкая (Y2=2)**.

##### Выход из строя аппаратно-программных средств

В Учреждении осуществляет резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Сбой системы электроснабжения

В Учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляет резервное копирование информации.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Стихийное бедствие

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

#### Угрозы преднамеренных действий внутренних нарушителей

##### Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

В Учреждении пользователи осведомлены о порядке работы с персональными данными.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

#### Угрозы несанкционированного доступа по каналам связи

##### Угроза «Анализ сетевого трафика»

##### Перехват за переделами контролируемой зоны.

Вероятность реализации угрозы – **низкая (Y2=2)**.

##### Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угроза «сканирование сети»

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угроза выявления паролей

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угрозы навязывание ложного маршрута сети

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угрозы подмены доверенного объекта

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Внедрение ложного объекта сети

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угрозы типа «Отказ в обслуживании»

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угрозы удаленного запуска приложений

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

##### Угрозы внедрения по сети вредоносных программ

Вероятность реализации угрозы – **маловероятна (Y2=0)**.

## Реализуемость угроз

Оценка реализуемости УБПДн представлена в таблице.

Таблица 3 – Реализуемость УБПДн

Все, что выделено цветом соответственно смотрим МЕТОДИКУ и считаем по формуле )

| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| --- | --- | --- |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.2. Угрозы утечки видовой информации | 0,5 | Средняя |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0,75 | Высокая |
| 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 | 0,5 | Средняя |
| 2.1.2. Кража носителей информации | 0,5 | Средняя |
| 2.1.3. Кража ключей и атрибутов доступа | 0,5 | Средняя |
| 2.1.4. Кражи, модификации, уничтожения информации | 0,5 | Средняя |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 0,5 | Средняя |
| 2.1.6. Несанкционированное отключение средств защиты | 0,6 | Средняя |
| 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) | 0,6 | Средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 0,5 | Средняя |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 0,6 | Средняя |
| 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 | 0,6 | Средняя |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 0,5 | Средняя |
| 2.3.3. Непреднамеренное отключение средств защиты | 0,6 | Средняя |
| 2.3.4. Выход из строя аппаратно-программных средств | 0,5 | Средняя |
| 2.3.5. Сбой системы электроснабжения | 0,5 | Средняя |
| 2.3.6. Стихийное бедствие | 0,5 | Средняя |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | 0,5 | Средняя |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | 0,5 | Средняя |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | | |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | 0,5 | Средняя |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | 0,6 | Средняя |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | 0,5 | Средняя |
| 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. | 0,5 | Средняя |
| 2.5.3.Угрозы выявления паролей по сети | 0,5 | Средняя |
| 2.5.4.Угрозы навязывание ложного маршрута сети | 0,5 | Средняя |
| 2.5.5.Угрозы подмены доверенного объекта в сети | 0,5 | Средняя |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,5 | Средняя |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | 0,5 | Средняя |
| 2.5.8.Угрозы удаленного запуска приложений | 0,5 | Средняя |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | 0,5 | Средняя |

## 

## Оценка опасности угроз

Оценка опасности УБПДн представлена таблице.

Таблица 4 – Опасность УБПДн

Все что выделено цветом соответственно смотрим МЕТОДИКУ и определяем ЭКСПЕРТНО т.е. самостоятельно:

* низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных
* средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
* высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

| **Тип угроз безопасности ПДн** | **Опасность угрозы** |
| --- | --- |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки видовой информации | Низкая |
| 1.2. 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 | Низкая |
| 2.1.2. Кража носителей информации | Низкая |
| 2.1.3. Кража ключей и атрибутов доступа | Низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | Низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| 2.1.6. Несанкционированное отключение средств защиты | Средняя |
| 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) | Низкая |
| 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 | Средняя |
| 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 | Низкая |
| 2.3.3. Непреднамеренное отключение средств защиты | Средняя |
| 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, не допущенными к ее обработке | Средняя |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Средняя |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | Низкая |
| 2.5.1.1. Перехват за переделами контролируемой зоны | Низкая |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | Низкая |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | 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 навязывание ложного маршрута сети | Низкая |
| 2.5.5.Угрозы подмены доверенного объекта в сети | Низкая |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | Низкая |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | Низкая |
| 2.5.8.Угрозы удаленного запуска приложений | Низкая |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | Низкая |

## Определение актуальности угроз в ИСПДн

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 5 – Актуальность УБПДн

Все что выделено цветом соответственно смотрим МЕТОДИКУ и определяем по таблице

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

| **Тип угроз безопасности ПДн** | **Актуальность угрозы** |
| --- | --- |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки видовой информации | неактуальная |
| 1.2. Угрозы утечки информации по каналам ПЭМИН | **актуальная** |
| 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 | неактуальная |
| 2.1.2. Кража носителей информации | неактуальная |
| 2.1.3. Кража ключей и атрибутов доступа | неактуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | неактуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | неактуальная |
| 2.1.6. Несанкционированное отключение средств защиты | **актуальная** |
| 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) | неактуальная |
| 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 | неактуальная |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | неактуальная |
| 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 лиц не допущенных к ее обработке | **актуальная** |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | **актуальная** |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | неактуальная |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | неактуальная |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | неактуальная |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | неактуальная |
| 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. | неактуальная |
| 2.5.3.Угрозы выявления паролей по сети | неактуальная |
| 2.5.4.Угрозы навязывание ложного маршрута сети | неактуальная |
| 2.5.5.Угрозы подмены доверенного объекта в сети | неактуальная |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | неактуальная |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | неактуальная |
| 2.5.8.Угрозы удаленного запуска приложений | неактуальная |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | неактуальная |

Были выявлены следующие актуальные угрозы:

1. Угрозы утечки информации по каналам ПЭМИН;
2. Несанкционированное отключение средств защиты;
3. Установка ПО не связанного с исполнением служебных обязанностей;
4. Непреднамеренное отключение средств защиты;
5. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;
6. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.