|  |  |  |
| --- | --- | --- |
| **ХАЛЬМГ ТАНГЧИН****БАh - ДθРВДЭ РАЙОНА****МУНИЦИПАЛЬН БУРДЭЦИН****АДМИНИСТРАЦИН ТОГТАВР** |  | **ПОСТАНОВЛЕНИЕ****АДМИНИСТРАЦИИ МАЛОДЕРБЕТОВСКОГО РАЙОННОГО МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ****РЕСПУБЛИКИ КАЛМЫКИЯ** |
|  |

с. Малые Дербеты № 83 от « 02 » октября 2014г.

Об утверждении частной модели угроз

безопасности персональных данных

при их обработке в информационной

системе персональных данных

администрации Малодербетовского

районного муниципального

образования Республики Калмыкия

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»

ПОСТАНОВЛЯЮ:

1. Утвердить частную модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных администрации Малодербетовского районного муниципального образования Республики Калмыкия.
2. Контроль над исполнением данного постановления возложить на заместителя Главы администрации Малодербетовского районного муниципального образования Республики Калмыкия – С.А. Базырова.

Глава администрации Г. Золочевский

Караваева о.

УТВЕРЖДАЮ

Глава администрации

Малодербетовского РМО РК

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г. Золочевский

« 02 » октября 2014 г.

|  |
| --- |
| **Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных администрации Малодербетовского районного муниципального образования Республики Калмыкия** |
| СОГЛАСОВАНО\* |

**1. Обозначения и сокращения**

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

АВС – антивирусные средства;

ВП – выделенное помещение;

ВТСС – вспомогательные технические средства и системы;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

МЭ – межсетевой экран;

НДВ – не декларированные возможности;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных:

СОВ – система обнаружения вторжений;

СУБД – система управления базами данных;

УБПДн – угрозы безопасности персональным данным

**2. Определения**

В настоящем документе используются следующие термины и их определения:

**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 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 к информации** - возможность получения информации и ее использования.

**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.

**Информационная система персональных данных** - 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 так средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

**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.

**Контролируемая зона -** пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание е сторонних 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.

**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.

**Оператор -** государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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).

**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.

**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 программу с целью осуществить утечку, изменить, блокировать, уничтожать 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.

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

**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.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации

от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уполномоченное оператором лицо** - лицо, которому на основании до­говора оператор поручает обработку персональных данных.

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

3 Введение

Частная модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн построена на основании методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

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

Анализ угроз безопасности персональных данных включает:

* описание угроз;
* оценку вероятности возникновения угроз;
* оценку реализуемости угроз;
* оценку опасности угроз;
* определение актуальности угроз.

## 4.1. Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

1.                 Фамилия, имя, отчество

2.                 Пол

3.                 Дата рождения

4.                 Место рождения

5.                 Адрес места жительства

6.                 Семейное положение

7.                 Сведения о месте работы или учебы членов семьи и родственников

8.                 Социальное положение

9.                 Имущественное положение

10.            Сведения о доходах, информации о выплатах и удержаниях

11.            Образование

12.            Профессия

13.            Сведения о документах, удостоверяющих личность

14.            Реквизиты ИНН

15.            Реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС)

16.            Реквизиты полиса обязательного медицинского страхования

17.            Сведения о трудовой деятельности, в том числе о стаже работы

18.            Сведения о социальных льготах

19.            Сведения о воинском учете

20.            Контактные телефоны (домашний, мобильный)

21.            Сведения о званиях и чинах

22.            Общие сведения о состоянии здоровья

23.            Фотография

24. Другие сведения содержащие персональные данные

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **\_\_3\_\_ категории персональных данных**.

Объем обрабатываемых персональных данных, не превышает записей о субъектах персональных данных.

## 4.2. Режим обработки ПДн

В ИСПДн обработка персональных данных осуществляется в однопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с ПДн: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

Таблица 1 – Матрица доступа

|  |  |  |
| --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия |
| Ответственные за обеспечение безопасности ПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств. Обладает правами оператора ИСПДн с правом «только чтение». | * использование
* блокировка
 |
| Операторы ИСПДн с правами записи | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.Располагает конфиденциальными данными, к которым имеет доступ | сборсистематизациянакоплениекопированиехранениеуточнениеиспользованиеблокировкауничтожение |
| Операторы ИСПДн с правами чтения | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | * использование
 |

## 4.3 Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

* внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
* внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

###  Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

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 утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

### Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с утвержденным положением о разграничении прав доступа к обрабатываемым ПДн в ИСПДн. К внутренним нарушителям могут относиться:

* администраторы ИСПДн (категория I);
* администраторы конкретных подсистем или баз данных ИСПДн (категория II);
* пользователи ИСПДн (категория III);
* пользователи, являющиеся внешними по отношению к конкретной ИСПДн (категория IV);
* лица, обладающие возможностью доступа к системе передачи данных (категория V);
* сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
* обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.) (категория VII);
* уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы 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.

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II 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 в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

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

### Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

* *общая информация* – информации о назначения и общих характеристиках ИСПДн;
* *эксплуатационная информация –* информация, полученная из эксплуатационной документации;
* *чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

* данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
* сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
* данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
* данные о реализованных в СЗПДн принципах и алгоритмах;
* исходные тексты программного обеспечения ИСПДн;
* сведения о возможных каналах реализации угроз;
* информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в ИСПДн, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИСПДн, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в ИСПДн.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об ИСПДн являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, 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, например, относится парольная, аутентифицирующая и ключевая информация.

### Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

* аппаратные компоненты СЗПДн;
* доступные в свободной продаже технические средства и программное обеспечение;
* специально разработанные 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 реализованные конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

* средств перехвата в технических каналах утечки;
* средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
* средств воздействия на источники и через цепи питания;
* средств воздействия через цепи заземления;
* средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

## 4.4 Исходный уровень защищенности ИСПДн

(Уровень исходной защищенности ИСПДн определяется на основании методического документа ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».)

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

В таблице 3 представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица – Показатели исходной защищенности ИСПДн

| **Технические и эксплуатационные характеристики ИСПДн** | **Уровень защищенности** |
| --- | --- |
| **Высокий** | **Средний** | **Низкий** |
| *1. По территориальному размещению:*распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | - |
| *1. По территориальному размещению:* |  |  |  |
|  |  |  |  |
| локальная ИСПДн, развернутая в пределах одного здания | + | – | – |
| *2. По наличию соединения с сетями общего пользования:* |  |  |  |
| ИСПДн, физически отделенная от сети общего пользования | + | – | – |
| *3. По встроенным (легальным) операциям с записями баз персональных данных:* |  |  |  |
|  |  |  |  |
| модификация, передача | – | – | + |
| *4. По разграничению доступа к персональным данным:* | – | + | – |
| ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; |  |  |  |
|  |
|  |  |  |  |
| *5. По наличию соединений с другими базами ПДн иных ИСПДн:* |  |  |  |
| ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | + | – | – |
| *6. По уровню обобщения (обезличивания) ПДн:*ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | - | – | + |
| *7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:* |  |  |  |
| ИСПДн, предоставляющая часть ПДн; | – | + | – |
|  |  |  |  |
|  |  |  |  |

Характеристика ИСПДн по уровням 42,8 28,6 28,6

Таким образом, ИСПДн имеет **средний уровень защищенности**.

## 4.5 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).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

### 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.

Вероятность реализации угрозы – **0***.*

### 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.

Вероятность реализации угрозы – **0***.*

### Угрозы утечки информации по каналам ПЭМИН

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

Вероятность реализации угрозы – **0***.*

### Угрозы несанкционированного доступа к информации

Угрозы доступа (проникновения) в операционную среду компьютера и НСД к персональным данным (угрозы непосредственного доступа):

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

* нарушению конфиденциальности (копирование, неправомерное рас­пространение);
* нарушению целостности (уничтожение, изменение);
* нарушению доступности (блокирование).

**Вероятность реализации угрозы – 2*.***

### 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.

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

Вероятность реализации угрозы – **2***.*

##### Кража ключей и атрибутов доступа

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

Вероятность реализации угрозы – **2***.*

##### 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.

Вероятность реализации угрозы – **2***.*

##### 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.

Вероятность реализации угрозы – **2***.*

##### Несанкционированное отключение средств защиты

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

Вероятность реализации угрозы – **2***.*

### Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа 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.

Вероятность реализации угрозы – **2***.*

##### 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.

Вероятность реализации угрозы – **0***.*

##### 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 характера**

Вероятность реализации угрозы **– 2*.***

##### 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.

Вероятность реализации угрозы – **2***.*

##### 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.

Вероятность реализации угрозы – **2***.*

##### 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.

Вероятность реализации угрозы – **2***.*

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

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

Вероятность реализации угрозы – **2***.*

##### Сбой системы электроснабжения

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

Вероятность реализации угрозы – **2***.*

**Угрозы преднамеренных действий внутренних нарушителей**

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

Угроза осуществляется путем НСД внешних пользователей к элементам ИСПДн.

Вероятность реализации угрозы – **0***.*

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

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении защищаемой информации.

Вероятность реализации угрозы – **2**.

**Угрозы несанкционированного доступа по каналам связи** (для распределенных ИСПДн)

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 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»с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации

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.

Вероятность реализации угрозы – **0***.*

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

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.

Вероятность реализации угрозы – **\_0\_**.

##### Угрозы выявления паролей по сети

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.

Вероятность реализации угрозы – **\_2**

##### 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.

Вероятность реализации угрозы – **\_0\_**.

##### Угрозы подмены доверенного объекта в сети

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.

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.

Вероятность реализации угрозы – **\_0\_**.

##### Угрозы внедрения 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, 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.

Вероятность реализации угрозы – **\_0\_**.

##### 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 запросов на установ­ление TCP-соединений, 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 сообщений почтовому серверу;
* 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 или идентификационной и аутентификационной информации;
* явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами или имеющих длину, превышающую макси­мально допустимый размер, 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.

Вероятность реализации угрозы – **\_0\_**.

##### 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 виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов; 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), либо штатными средствами управления и администрирования компьютерных се­тей. В результа­те их использования удается добиться удаленного контроля над станцией в сети.

Вероятность реализации угрозы – **\_0\_**.

##### 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.

Вероятность реализации угрозы – **\_0\_**.

**4.6 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 реализуемости УБПДн представлена в таблице 4.

Таблица 3 – Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| 1. Угрозы от утечки по техническим каналам. |
| 1.1. Угрозы утечки акустической информации | 0 | Н |
| 1.2. Угрозы утечки видовой информации | 0 | Н |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0 | Н |
| 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 | 0,1 | Н |
| 2.1.2. Кража носителей информации | 0 | Н |
| 2.1.3. Кража ключей и атрибутов доступа | 0,1 | Н |
| 2.1.4. Кражи, модификации, уничтожения информации | 0,1 | Н |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 0,1 | Н |
| 2.1.6. Несанкционированное отключение средств защиты | 0,1 | Н |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) |
| 2.2.1. Действия вредоносных программ (вирусов) | 0,1 | С |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 0 | Н |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 0 | Н |
| 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 характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания). |
| 2.3.1. Утрата ключей и атрибутов доступа | 0,1 | Н |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 0,1 | Н |
| 2.3.3. Непреднамеренное отключение средств защиты | 0,1 | Н |
| 2.3.4. Выход из строя аппаратно-программных средств | 0,1 | Н |
| 2.3.5. Сбой системы электроснабжения | 0,1 | Н |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 0 | Н |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 0,1 | Н |
| 2.5.Угрозы несанкционированного доступа по каналам связи |
| 2.5.1.Угроза «Анализ сетевого трафика» | 0 | Н  |
| 2.5.1.1. Перехват за переделами контролируемой зоны | 0 | Н  |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | 0 | Н  |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями | 0,1 | Н  |
| 2.5.2.Угрозы сканирования сети | 0 | Н  |
| 2.5.3.Угрозы выявления паролей по сети | 0 | Н  |
| 2.5.4.Угрозы навязывание ложного маршрута сети | 0 | Н  |
| 2.5.5.Угрозы подмены доверенного объекта в сети | 0 | Н  |
| 2.5.6.Угрозы внедрения ложного объекта как в сети | 0 |  Н |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | 0 | Н  |
| 2.5.8.Угрозы удаленного запуска приложений | 0 | Н  |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | 0 | Н  |

**4.7. 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.

Оценка опасности УБПДн представлена таблице 5.

Таблица 5 – Опасность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасностьугрозы |
| 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 | 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 | низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа 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 | низкая |
| 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 характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) |
| 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 | низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | низкая |
| 2.3.5. Сбой системы электроснабжения | низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | низкая |
| 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» | низкая |
| 2.5.1.1. Перехват за переделами с 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 сети | 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 в сети | 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 |

**4.8 Определение актуальности угроз в ИСПДн**

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

Таблица 6 – 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 |

Оценка актуальности угроз безопасности представлена в таблице 7.

Таблица 7 – Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасностьугрозы |
| 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 | 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 | 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) | низкая |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | низкая |
| 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 характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) |
| 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 | низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | низкая |
| 2.3.5. Сбой системы электроснабжения | низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | низкая |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | низкая |
| 2.5.Угрозы несанкционированного доступа по каналам связи. |
| 2.5.1.Угроза «Анализ сетевого трафика» | 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 сети | 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 сети | 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 |

## 4.9. **М**одель угроз безопасности ПДн при их обработке в ИСПДн (наименование ИСПДн) (сводная таблица)

## Исходный класс защищенности – К\_2\_\_\_.

Таблица 8 – Угрозы безопасности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе |
| Организационно-технические |
| 1. Угрозы от утечки по техническим каналам |
| 1.1. Угрозы утечки акустической информации | 0 | н | н | н |  |
| 1.2. Угрозы утечки видовой информации | 0 | н | н | н |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0 | н | н | н |
| 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 | н | в | а | Организация пропускного режима.Контроль доступа в помещения, где ведется обработка ПДн.Вменение персоналу ИСПДн обязанности обеспечения сохранности носителей информации, содержащих ПДн. |
| 2.1.2. Кража носителей информации | 2 | н | н | н | Организация пропускного режима.Контроль доступа в помещения, где ведется обработка ПДн.Организация выполнения работ технического обслуживания, выполняемых работниками сторонних организаций, в присутствии работников организации.Включение требования по информационной безопасности в договоры и контракты на проведение работ и оказание услуг.Выбор в качестве исполнителей работ и поставщиков услуг организаций, прошедших сертификацию.Заключение соглашений о конфиденциальности со сторонними организациями, выполняющими работы или оказывающими услуги. |
| 2.1.3. Кража ключей и атрибутов доступа | 2 | н | с | н |
| 2.1.4. Кражи, модификации, уничтожения информации | 2 | н | с | н |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 2 | н | н | н |
| 2.1.6. Несанкционированное отключение средств защиты | 2 | н | н | н |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) |
| 2.2.1. Действия вредоносных программ (вирусов) | 2 | с | н | н | Использование на серверах и АРМ, входящих в состав ИСПДн, антивирусного ПО.Выполнение регулярного обновления ПО АРМ и серверов ИСПДн.Настройка антивирусного ПО на проверку подключаемых отчуждаемых носителей информации. |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 0 | н | н | н |  |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 2 | н | н | н | Запрет установки ПО, не связанного с исполнением служебных обязанностей.Регулярный контроль со стороны работников, ответственных за обеспечение безопасности ПДн при их обработке в ИСПДн, прав доступа пользователей к АРМ и установленного на них ПО. |
| 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 характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) |
| 2.3.1. Утрата ключей и атрибутов доступа | 2 | н | н | н | Организация пропускного режима.Контроль доступа в помещения, где ведется обработка ПДн.Вменение персоналу ИСПДн обязанности обеспечения сохранности носителей информации, содержащих ПДн. |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 2 | н | н | н | Резервное копирование данных ИСПДн.Хранение резервных копий отдельно от элементов ИСПДн, содержащих резервируемые данные.Использование в серверных помещениях средств обнаружения возгорания и систем пожаротушения.Установка резервных источников электропитания |
| 2.3.3. Непреднамеренное отключение средств защиты | 2 | н | н | н |
| 2.3.4. Выход из строя аппаратно-программных средств | 2 | н | н | н |
| 2.3.5. Сбой системы электроснабжения | 2 | н | н | н |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке | 2 | н | н | н | Организация пропускного режима.Контроль доступа в помещения, где ведется обработка ПДн.Организация выполнения работ технического обслуживания, выполняемых работниками сторонних организаций, в присутствии работников организации.Включение требования по информационной безопасности в договоры и контракты на проведение работ и оказание услуг.Выбор в качестве исполнителей работ и поставщиков услуг организаций, прошедших сертификацию.Заключение соглашений о конфиденциальности со сторонними организациями, выполняющими работы или оказывающими услуги. |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | 2 | н | с | н | Усиление контроля за сотрудниками имеющими доступ к ПД |
| 2.5. Угрозы несанкционированного доступа по каналам связи |
| 2.5.1. Угроза «Анализ сетевого трафика» | 0 | н | н | н |  |
| 2.5.1.1. Перехват за переделами контролируемой зоны | 0 | н | н | н |  |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | 0 | н | н | н |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями | 2 | н | с | н |  |
| 2.5.2.Угрозы сканирование сети | 0 | н | н | н |  |
| 2.5.3. Угрозы выявления паролей по сети | 0 | н | н | н |  |
| 2.5.4. Угрозы навязывание ложного маршрута сети | 0 | н | н | н |  |
| 2.5.5. Угрозы подмены доверенного объекта в сети | 0 | н | н | н |  |
| 2.5.6. Угрозы внедрения ложного объекта в сети | 0 | н | н | н |  |
| 2.5.7. Угрозы типа «Отказ в обслуживании» | 0 | н | н | н |  |
| 2.5.8. Угрозы удаленного запуска приложений | 0 | н | н | н |  |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | 0 | н | н | н |  |

## 4. Структура ИСПДн

Таблица 4 – Параметры ИСПДн

|  |  |
| --- | --- |
| Количество рабочих станций, входящих в состав ИСПДн | 4 |
| Структура ИСПДн | Автономная  |
| Количество пользователей, допущенных к работе в ИСПДн | 4 |
| Режим обработки ПДн в ИСПДн | однопользовательский  |
| Подключение ИСПДн к локальным (распределенным) сетям общего пользования | Не имеется |
| Подключение ИСПДн к сетям международного информационного обмена | Не имеется |
| Тип ИСПДн | Типовая |
| Местонахождение технических средств ИСПДн | Все технические средства ИСПДн находятся в пределах Российской Федерации |