**Муниципальное учреждение «Местная администрация сельского поселения Эльбрус»**

**Эльбрусского муниципального района Кабардино-Балкарской Республики**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ПОСТАНОВЛЕНИЕ**

**«09» июля 2018 г. № 130**

**Об утверждении частной модели угроз безопасности персональных данных**

**при их обработке в информационной системе персональных данных**

**местной администрации сельского поселения Эльбрус**

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

 **ПОСТАНОВЛЯЮ:**

1. Утвердить частную модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных местной администрации сельского поселения Эльбрус (прилагается).

2. Контроль за исполнением настоящего постановления возложить на первого заместителя главы местной администрации сельского поселения Эльбрус - И. И. Афашокову.

# Глава сельского поселения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_М. З. Согаев

**Начальник правового отдела \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.А. Барасбиев**

Утверждена

постановлением местной администрации

сельского поселения Эльбрус

«09» июля 2018 г. № 130

Частная модель угроз безопасности персональных данных

при их обработке в информационной системе персональных данных

местной администрации сельского поселения Эльбрус

**Сокращения**

АВС – антивирусные средства

АС – автоматизированная система

АРМ – автоматизированное рабочее место

БД – база данных

ВТСС – вспомогательные технические средства и системы

ИКХ – информация конфиденциального характера

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

НСД – несанкционированный доступ к информации

МЭ – межсетевой экран

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ППО – прикладное программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средство защиты информации

СЗПДн – система защиты персональных данных

СОВ – система обнаружения вторжений

СФ – среда функционирования

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

**Термины и определения**

**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 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, 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).

**1 Введение.**

Настоящий документ подготовлен в рамках выполнения работ по построению системы защиты персональных данных (далее – СЗПДн), не содержащей сведений, составляющих государственную тайну, информационной системы персональных данных местной администрации сельского поселения Эльбрус (далее - ИСПДн).

 Настоящий документ содержит модель угроз безопасности персональных данных для ИСПДн (далее – модель угроз).

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации ИСПДн и проектирования СЗПДн.

Модель угроз – документ, использующийся для:

* анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
* разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
* проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
* недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
* контроля обеспечения уровня защищенности персональных данных.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку 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.

Модель угроз для ИСПДн разрабатывается в соответствии со следующими нормативными и методологическими документами:

* Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
* Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
* Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462);
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

В процессе развития СЗПДн предполагается конкретизировать и пересматривать модель угроз для ИСПДн.

Модель угроз может быть пересмотрена:

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

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

При разработке модели угроз для ИСПДн учитывается, что СЗПДн является специальной информационной системой т.к., к обрабатываемым в ней данным предъявляются требования не только по конфиденциальности, но и по целостности и доступности.

**2 Назначение, структура и основные характеристики ИСПДн.**

Рассматриваемые ИСПДн имеет подключение к сетям общего пользования и международного обмена.

Все компоненты ИСПДн находятся на объектах вычислительной техники внутри контролируемой зоны.

Обработка персональных данных в местной администрации сельского поселения Эльбрус ведется в многопользовательском режиме с разграничением прав доступа.

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

Основные параметры ИСПДн приведены в таблице 1.

Таблица 1 – Параметры ИСПДн

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

В ИСПД обрабатываются следующие типы ПДн:

* фамилия, имя, отчество;
* год, месяц, дата и место рождения;
* адрес проживания;
* номер паспорта;
* должность;
* заработная плата;
* ИНН;
* № страхового пенсионного свидетельства.

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

Объем обрабатываемых персональных данных, не превышает 1000 записей о субъектах персональных данных.

Для функционирования прикладных программ в состав ИСПДн входит следующее специальное оборудование:

* МФУ, подключенный к разъему USB системного блока.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. Местная администрация сельского поселения Эльбрус располагает необходимыми данными для идентификации, аутентификации, а также препятствует несанкционированному доступу к ресурсам.

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

Таблица 2 – Матрица доступа

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия | Сотрудники отдела |
| Администратор безопасности | 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. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор- систематизация- накопление- хранение- уточнение- использование- уничтожение | Сотрудник отдела защиты информации |
| Операторы ИСПДн с правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор- систематизация- накопление- хранение- уточнение- использование- уничтожение | Управляющий делами главы местной администрации сельского поселения Эльбрус, бухгалтера, архивариус |

**3 Модель вероятного нарушителя информационной безопасности.**

**3.1 Описание возможных нарушителей**

Все нарушители делятся на две группы:

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

**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 несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

* администраторы ИСПДн (категория I);
* пользователи ИСПДн (категория II);
* сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИСПДн, но не имеющие права доступа к ресурсам (категория III);
* обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория IV);
* уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория V).

На лиц I категории 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, используемые в конкретных АС, 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 (например, программное обеспечение, полученное из общедоступных внешних источников).

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

На лиц II категории возложены задачи по использованию программно-аппаратных средств и баз данных ИСПДн. Пользователи 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, используемые в конкретных АС, в соответствии с установленными для них полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационных 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-V относятся к вероятным нарушителям.

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

**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.

К внешним нарушителям могут относиться:

* бывшие сотрудники – администраторы или пользователи ИСПД (категория VI);
* посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке (категория VII).

Лица категории VI 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 (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категории VII могут быть знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, но не знакомы с применяемыми принципами и концепциями безопасности на объекте ИСПД. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категорий VI и VII потенциально могут реализовывать угрозы ИБ, используя возможности по несанкционированному доступу к защищаемой информации по каналам связи, обрабатываемой и хранимой в ИСПДн.

Предполагается, что лица категорий VI и VII относятся к вероятным нарушителям.

**3.2 Предположения об имеющейся у нарушителя информации об объектах реализации угроз.**

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

* информации о назначения и общих характеристиках ИСПДн;
* информация, полученная из эксплуатационной документации;
* 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 СЗИ принципах и алгоритмах;
* исходные тексты программного обеспечения ИСПДн;
* сведения о возможных каналах реализации угроз;
* информацию о способах реализации угроз.

Предполагается, что лица категорий III - VII не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категорий V – VI обладают чувствительной информацией об ИСПДн и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ИСПДн.

Организационными мерами предполагается исключить доступ лиц категории V к техническим и программным средствам ИСПД в момент обработки с использованием этих средств защищаемой информации.

Предполагается полностью исключить доступ лиц категорий VI – VII к техническим и программным средствам ИСПД.

Таким образом, наиболее информированными об АС являются лица категорий V – VI.

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 необходимых условий безопасности персональных данных 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.

**3.3. Предположения об имеющихся у нарушителя средствах реализации угроз.**

Предполагается, что нарушитель имеет:

* аппаратные компоненты СЗПДн и СФ СЗПДн;
* доступные в свободной продаже технические средства и программное обеспечение.

Предполагается что содержание и объем персональных данных, находящихся в ИСПДн не достаточны для мотивации применения нарушителем специально разработанных технических средства и программного обеспечения.

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 на объекте ИСПДн 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 определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, доступные в свободной продаже, 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 V-VII.

**3.4. Описание объектов и целей реализации угроз информационной безопасности.**

Основными информационными ресурсами, обрабатываемыми в ИСПД являются следующие:

1. Целевая информация:

* персональные данные сотрудников;

2. Технологическая информация:

* защищаемая управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
* защищаемая технологическая информация средств доступа к системам управления ИСПДн (аутентификационная информация и др.);
* информационные ресурсы на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами ИСПДн (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
* информация о СЗПДн, их структуре, принципах и технических решениях защиты;
* информационные ресурсы ИСПДн (базы данных и файлы), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах.

3. Программное обеспечение:

* программные информационные ресурсы ИСПДн, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами ИСПДн, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств защиты.

Предполагается, что не являются объектами реализации угроз:

* технические каналы утечки информации;
* сигнальные цепи (информационные и управляющие интерфейсы СВТ);
* источники и цепи электропитания;
* цепи заземления.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

**3.5 Описание каналов реализации угроз информационной безопасности.**

Возможными каналами реализации угроз информационной безопасности являются:

* каналы доступа, образованные с использованием специально разработанных технических средств и программного обеспечения.

Предполагается, что не являются каналами реализации угроз:

* технические каналы утечки;
* сигнальные цепи;
* источники и цепи электропитания;
* цепи заземления;
* каналы активного воздействия на технические средства с помощью облучения.

**3.6 Основные способы реализации угроз информационной безопасности.**

При определении основных способов реализации угроз информационной безопасности ресурсов ИСПДн, учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла ИСПДн, компонентов, условий функционирования ИСПДн, а также - предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности ИСПДн:

1) несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн и недостатков механизмов разграничения доступа;

2) негативные воздействия на программно-технические компоненты ИСПДн вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;

3) маскировка под администратора ИСПДн, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых ИСПДн;

4) осуществление прямого хищения (утраты) элементов ИСПДн, носителей информации и производственных отходов (распечаток, списанных носителей);

5) компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых ИСПДн;

6) методы социальной инженерии для получения сведений об ИСПДн, способствующих созданию благоприятных условий для применения других методов;

7) использование оставленных без присмотра незаблокированных средств администрирования ИСПДн и АРМ;

8) сбои и отказы программно-технических компонентов ИСПДн;

9) внесение неисправностей, уничтожение технических и программно-технических компонентов ИСПДн путем непосредственного физического воздействия;

10) осуществление несанкционированного доступа к информации при ее передаче.

##

## 4. 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.

Таблица 3 – Исходный уровень защищенности

|  |  |  |
| --- | --- | --- |
| Позиция | Технические и эксплуатационные характеристики | Уровеньзащищенности |
| 1 | По территориальному размещению | Высокий |
| 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 | Высокая |

ИСПДн имеет *средний* уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности Y1 =5.

**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:

###

### 5.1. Угрозы утечки информации по техническим каналам.

####

#### 5.1.1. 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 наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

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

Вероятность реализации угрозы – **маловероятна**.

####

#### 5.1.2. 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.

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, АРМ с ИСПДн расположены на первом этаже здания, окна выходят во двор контролируемой зоны так, что практически исключен визуальный просмотр посторонними лицами информации на мониторе. Вывод на печать ПДн осуществляется не чаще одного раза в год. Отпечатанные данные хранятся в сейфе.

Вероятность реализации угрозы – **маловероятна**.

####

#### 5.1.3 Угрозы утечки информации по каналам ПЭМИН.

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

Угрозы данного класса **маловероятны**, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся в на большом расстоянии от ее границы и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

###

### 5.2. Угрозы несанкционированного доступа к информации.

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).

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

#####

##### **5.2.1.1.Кража ПЭВМ.**

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

В здании местной администрации сельского поселения Эльбрус введен круглосуточный контроль доступа в контролируемую зону, который осуществляется охраной, двери закрываются на замок, ведется видеонаблюдение, вынос компьютерный техники за пределы здания возможен только по специальным пропускам.

Вероятность реализации угрозы – **маловероятной**.

#####

##### **5.2.1.2. Кража носителей информации.**

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

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы – **маловероятна**.

#####

##### **5.2.1.3. Кража ключей и атрибутов доступа.**

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

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и паролей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы – **маловероятна**.

#####

##### **5.2.1.4. 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.

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

#####

##### **5.2.1.5. 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.

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

**5.2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.**

В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы – **маловероятна**.

#####

##### **5.2.1.7. Несанкционированное отключение средств защиты.**

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

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – **низкая вероятность**.

#### 5.2.2. 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).

#####

##### **5.2.2.1. 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.

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

Вероятность реализации угрозы – **низкая вероятность**.

#####

##### **5.2.2.2. 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 – ***маловероятна***.

#####

##### **5.2.2.3. 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.

Все пользователи проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – **средняя вероятность**.

#### 5.2.3 .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.

##### **5.2.3.1. 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.

В местной администрации сельского поселения Эльбрус введена парольная политика, предусматривающая требуемую сложность пароля, 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 – **средняя вероятность**.

##### **5.2.3.2. 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.

В местной администрации сельского поселения Эльбрус осуществляется резервное копирование обрабатываемых ПДн.

Вероятность реализации угрозы – **средняя вероятность**.

##### **5.2.3.3. 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.

В местной администрации сельского поселения Эльбрус 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 – **маловероятна**.

##### **5.2.3.4. Выход из строя аппаратно-программных средств.**

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

В местной администрации сельского поселения Эльбрус осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **средняя вероятность**.

##### **5.2.3.5. Сбой системы электроснабжения.**

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

В местной администрации сельского поселения Эльбрус ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.3.6.Стихийное бедствие.**

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В местной администрации сельского поселения Эльбрус установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна**.

#### 5.2.4. Угрозы преднамеренных действий внутренних нарушителей.

##### **5.2.4.1. 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.

В здании местной администрации сельского поселения Эльбрус введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.4.2. 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.

В местной администрации сельского поселения Эльбрус пользователи осведомлены о порядке работы с персональными данными, а так же подписали Соглашение о неразглашении.

Вероятность реализации угрозы – **маловероятна**.

#### 5.2.5. 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.

##### **5.2.5.1. 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.

В местной администрации сельского поселения Эльбрус передача информации по каналам связи не осуществляется.

##### **Перехват за переделами контролируемой зоны.**

Вероятность реализации угрозы – **маловероятна**.

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

Вероятность реализации угрозы – **маловероятна**.

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

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.5.2. 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.

Вероятность реализации угрозы – **высокая вероятность**.

##### **5.2.5.3. 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.

В местной администрации сельского поселения Эльбрус применяются стойкие пароли. Пароли меняются с частотой один раз в месяц.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.5.4. 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.

В местной администрации сельского поселения Эльбрус не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.5.5. 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.

В местной администрации сельского поселения Эльбрус не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.5.6. 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.

В местной администрации сельского поселения Эльбрус не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

##### **5.2.5.7. 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.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

##### **5.2.5.8. 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.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

##### **5.2.5.9. 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.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

## 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.

Таблица 4 – 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 | 0,25 | низкая |
| 1.2. Угрозы утечки видовой информации | 0,25 | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0,25 | низкая |
| 2. Угрозы несанкционированного доступа к информации. |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн |
| 2.1.1. Кража ПЭВМ | 0,25 | низкая |
| 2.1.2. Кража носителей информации | 0,25 | низкая |
| 2.1.3. Кража ключей и атрибутов доступа | 0,25 | низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | 0,25 | низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 0,25 | низкая |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | 0,25 | низкая |
| 2.1.7. Несанкционированное отключение средств защиты | 0,35 | 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) | 0,35 | средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 0,25 | низкая |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 0,5 | 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 | 0,5 | средняя |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 0,75 | высокая |
| 2.3.3. Непреднамеренное отключение средств защиты | 0,25 | низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | 0,5 | средняя |
| 2.3.5. Сбой системы электроснабжения | 0,25 | низкая |
| 2.3.6. Стихийное бедствие | 0,25 | низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | 0,25 | низкая |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | 0,25 | низкая |
| 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: | 0,25 | низкая |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | 0,25 | низкая |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | 0,25 | низкая |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | 0,25 | 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. | 0,75 | высокая |
| 2.5.3.Угрозы выявления паролей по сети | 0,25 | низкая |
| 2.5.4.Угрозы навязывание ложного маршрута сети | 0,25 | низкая |
| 2.5.5.Угрозы подмены доверенного объекта в сети | 0,25 | низкая |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,25 | низкая |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | 0,25 | низкая |
| 2.5.8.Угрозы удаленного запуска приложений | 0,25 | низкая |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | 0,25 | низкая |

## 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.

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Низкая |
| 2.1.7. 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 (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 | Низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | Низкая |
| 2.3.5. Сбой системы электроснабжения | Низкая |
| 2.3.6. Стихийное бедствие | Низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных 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» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | 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, 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 |

## 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.

Таблица 7 – Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Актуальность угрозы |
| 1. Угрозы от утечки по техническим каналам. |
| 1.1. Угрозы утечки акустической информации | Не актуальная |
| 1.2. Угрозы утечки видовой информации | Не актуальная |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Не 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 | Не актуальная |
| 2.1.2. Кража носителей информации | Не актуальная |
| 2.1.3. Кража ключей и атрибутов доступа | Не актуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | Не актуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Не актуальная |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Не актуальная |
| 2.1.7. Несанкционированное отключение средств защиты | Не 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) | Не актуальная |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | Не актуальная |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | Не 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 | Не актуальная |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | Актуальная |
| 2.3.3. Непреднамеренное отключение средств защиты | Не актуальная |
| 2.3.4. Выход из строя аппаратно-программных средств | Не актуальная |
| 2.3.5. Сбой системы электроснабжения | Не актуальная |
| 2.3.6. Стихийное бедствие | Не актуальная |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | Не актуальная |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Не 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: | Не актуальная |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | Не актуальная |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | Не актуальная |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | Не актуальная |
| 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. | Актуальная |
| 2.5.3.Угрозы выявления паролей по сети | Не актуальная |
| 2.5.4.Угрозы навязывание ложного маршрута сети | Не актуальная |
| 2.5.5.Угрозы подмены доверенного объекта в сети | Не актуальная |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | Не актуальная |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | Не актуальная |
| 2.5.8.Угрозы удаленного запуска приложений | Не актуальная |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | Не актуальная |

Были выявлены следующие актуальные угрозы:

1. Непреднамеренная модификация (уничтожение) информации сотрудниками
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.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

1. Резервное копирование данных ИСПДн.
2. Установка межсетевого экрана

## 9. Модель угроз безопасности

Исходный класс защищенности – средний (Y1=5).

Таблица 8 – Угрозы безопасности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе |
| Технические | Организационные |
| 1. Угрозы от утечки по техническим каналам |
| 1.1. Угрозы утечки акустической информации | Маловероятна | Низкая | Низкая | Неактуальная |  | Инструкция пользователяТехнологический процесс |
| 1.2. Угрозы утечки видовой информации | Маловероятна | Низкая | Низкая | Неактуальная | Жалюзи на окнаРасположение монитора | Инструкция пользователяТехнологический процесс |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Маловероятна | Низкая | Низкая | Неактуальная |  |  |
| 2. Угрозы несанкционированного доступа к информации |  |  |  |  |
| 2.1. Угрозы уничтожения, хищения аппаратных средств испдн носителей информации путем физического доступа к элементам испдн |
| 2.1.1. Кража ПЭВМ | Маловероятна | Низкая | Низкая | Неактуальная |  | Пропускной режимОхрана |
| 2.1.2. Кража носителей информации | Маловероятна | Низкая | Низкая | Неактуальная | Хранение в сейфеШифрование данных при помощи ViPNet SafeDisk | Пропускной режимОхранаАкт установки средств защитыУчет носителей информацииИнструкция пользователя |
| 2.1.3. Кража ключей доступа | Маловероятна | Низкая | Низкая | Неактуальная | Хранение в сейфе | Инструкция пользователя |
|
| 2.1.4. Кражи, модификации, уничтожения информации. | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных при помощи ViPNet SafeDiskСистема защиты от НСД ViPNet Personal Firewall | Пропускной режимОхранаАкт установки средств защиты |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | Маловероятна | Низкая | Низкая | Неактуальная |  | Пропускной режимОхрана |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных при помощи ViPNet SafeDisk | Ремонт допущенными сотрудниками учреждения |
| 2.1.7. Несанкционированное отключение средств защиты | Низкая вероятность | Средняя | Низкая | Неактуальная | Настройка средств защиты | Инструкция администратора безопасностиТехнологический процесс обработки |
|  |
| 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 вероятность | Средняя | Низкая | Неактуальная | Антивирусная защита Security Studio Endpoint Protection | Инструкция пользователяИнструкция ответственногоИнструкция администратора безопасностиТехнологический процесс обработкиИнструкция по антивирусной защите |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | Маловероятна | Низкая | Низкая | Неактуальная | Настройка средств защиты | Приобретение у доверенной организации |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | Средняя вероятность | Средняя | Низкая | Неактуальная | Настройка средств защиты | Инструкция пользователяИнструкция ответственногоИнструкция администратора безопасностиТехнологический процесс обработки |
| 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 | Средняя вероятность | Средняя | Низкая | Неактуальная | Хранение в сейфе | Инструкция пользователяИнструкция администратора безопасностиЖурнал учета паролей |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | Высокая вероятность | Высокая | Низкая | Актуальная | Настройка средств защиты | Инструкция пользователя |
| 2.3.3. Непреднамеренное отключение средств защиты | Маловероятна | Низкая | Низкая | Неактуальная | Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасностиНастройка средств защиты | Инструкция пользователяИнструкция администратора безопасности Инструкция по антивирусной защите |
| 2.3.4. Выход из строя аппаратно-программных средств | Средняя вероятность | Средняя | Низкая | Неактуальная |  |  |
| 2.3.5. Сбой системы электроснабжения | Маловероятна | Низкая | Низкая | Неактуальная | Использование источника бесперебойного электропитания |  |
| 2.3.6. Стихийное бедствие | Маловероятна | Низкая | Низкая | Неактуальная | Пожарная сигнализация | Инструкция по действиям в случае возникновения нештатной ситуации |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |  |  |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке | Маловероятна | Низкая | Низкая | Неактуальная | Шифрование данных при помощи DALLAS LOCK 8.0-K, средства криптографической защиты информации Континент – АП. | Акт установки средств защитыРазрешительная система допускаТехнологический процесс обработки |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | Маловероятна | Низкая | Низкая | Неактуальная |  | Обязательство о не разглашенииИнструкция пользователя |
| 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; | Маловероятна | Низкая | Низкая | Неактуальная |  |  |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями; | Маловероятна | Низкая | Низкая | Неактуальная |  |  |
|  |  |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | Маловероятна | Низкая | Низкая | 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. | Высокая вероятность | Высокая | Низкая | Актуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.3. Угрозы выявления паролей по сети. | Маловероятна | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.4. Угрозы навязывание ложного маршрута сети. | Маловероятна | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.5. Угрозы подмены доверенного объекта в сети. | Маловероятна | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях. | Маловероятно | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.7. Угрозы типа «Отказ в обслуживании». | Маловероятно | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.8. Угрозы удаленного запуска приложений. | Маловероятно | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, |  |
| 2.5.9. Угрозы внедрения по сети вредоносных программ. | Маловероятно | Низкая | Низкая | Неактуальная | программный комплекс защиты информации при передаче по сети Vip Net Client, провайдер криптографических функций Vip Net CSP, Антивирусная защита Security Studio Endpoint Protection |  |

10. Заключение.

Ввиду исключительной роли в ИСПДн лиц категорий I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Лица категорий III-VII относятся к вероятным нарушителям.

Среди лиц категорий III-VII наиболее опасными вероятными нарушителями являются лица категорий V-VI (уполномоченный персонал разработчиков СЗПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов СЗПДн, бывшие сотрудники).

На основании проведенного анализа можно сделать вывод что вероятный нарушитель относится к классу Н1.

Представленная модель угроз для ИСПДн должна использоваться при формировании обоснованных требований информационной безопасности и проектировании ИСПД.

Для предотвращения возможности реализации актуальных угроз безопасности необходимо:

организовать резервное копирование информации, хранящейся в ИСПДн;

обеспечить защиту сетевого периметра АРМ с ИСПДн с помощью межсетевого экрана;

разработать инструкции пользователей ИСПДн.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, исходя из анализа угроз безопасности ПДн, а так же учитывая то, что: ИСПД является специальной информационной системой, в ИСПД одновременно обрабатываются данные менее 1000 субъектов персональных данных, нарушение безопасности персональных данных, обрабатываемых в ИСПД, может привести к незначительным негативным последствиям для субъектов персональных данных, класс информационной системы определяется по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных, можно определить, что ИСПДн классифицируется, как специальная ИСПДн класса K4.

Аттестация ИСПДн не требуется.