УТВЕРЖДЕНО
приказом МБУДО «Детская
музыкальная школа № 4» г. Кирова
от 01.10.2024 № 85-ОД

Модель
угроз безопасности персональных данных при их обработке в информационных системах персональных данных муниципального бюджетного учреждения дополнительного образования «Детская музыкальная школа №4» города Кирова

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
ВП	–	вредоносная программа
ВТСС	–	вспомогательные технические средства и системы
ИСПДн	–	информационная система персональных данных
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПО	–	программное обеспечение
ПДн	–	персональные данные
ПЭМИН	–	побочные электромагнитные излучения и наводки
СПД	–	сеть передачи данных
ЭВМ	–	электронно-вычислительная машина

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Доверенный объект сети – объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

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 таких средств.

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

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

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

Персональные данные – любая информация, относящаяся к определённому 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 и другая информация.

Программно-математическое воздействие – это несанкционированное воздействие на ресурсы автоматизированной информационной системы с помощью вредоносных программ.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

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

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – модель угроз) муниципального бюджетного учреждения дополнительного образования «Детская музыкальная школа №4» города Кирова (далее – модель Учреждения) разработана на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства РФ № 781 от 17 ноября 2007 г. и методических документов ФСТЭК России:

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Под угрозами безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (далее – угрозами) понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

Угрозы безопасности ПДн могут быть реализованы за счет утечки информации по техническим каналам (технические каналы утечки информации, обрабатываемой ЭВМ, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации), либо за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения.

Актуальной считается угроза, которая может быть реализована в информационной системе персональных данных (ИСПДн) и представляет опасность для ПДн. Порядок определения актуальных угроз безопасности ПДн в ИСПДн определяется документом «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

НАЗНАЧЕНИЕ МОДЕЛИ УГРОЗ

Настоящая модель угроз разрабатывается для определения возможных угроз и опасности для ПДн в случае их реализации. Целью разработки является формирование перечня актуальных угроз для ИСПДн.

С использованием данных о классе ИСПДн и перечня актуальных угроз, на основе документа ФСТЭК России «Положение о методах и способах защиты информации в информационных системах персональных данных», формируются конкретные организационно-технические требования по защите информации ИСПДн от утечки информации по техническим каналам и от несанкционированного доступа, а также осуществляется выбор средств защиты.

Настоящая модель угроз может быть пересмотрена:

– по решению оператора при изменениях расположения, конфигурации, режима функционирования ИСПДн и т.п.;

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

УРОВЕНЬ ИСХОДНОЙ ЗАЩИЩЕННОСТИ ИСПДН

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

В настоящей модели угроз приведена информация для ИСПДн, функционирующей на базе единой структурированной кабельной сети общеобразовательного учреждения центра образования Кировского района Санкт-Петербурга «Центр информационной культуры»:

– Информационная система «ПараГраф: Район» (ИСПДн «ПараГраф: Район»).

Таблица 1 – Показатели исходной защищенности ИСПДн «ПараГраф: Район»

Технические и эксплуатационные характеристики ИСПДн «ПараГраф: Район»	**Уровни защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:	+	□	□

- локальная ИСПДн, развернутая в пределах одного здания			
2. По наличию соединения с сетями общего пользования: - ИСПДн, имеющая одноточечный выход в сеть общего пользования	□	+	□
3. По встроенным (легальным) операциям с записями баз персональных данных: - модификация, передача	□	□	+
4. По разграничению доступа к персональным данным: - ИСПДн, к которой имеет доступ определенный перечень сотрудников 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	□	+	□
Процентное соотношение	**28**	**44**	**28**

ИСПДн «ПараГраф: Район» имеет ***средний*** уровень исходной защищенности, т.к. не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний".

При составлении перечня актуальных угроз ПДн низкому уровню исходной защищенности ставится в соответствие числовой коэффициент Y1 равный 5.

ЧАСТОТА (ВЕРОЯТНОСТЬ) РЕАЛИЗАЦИИ УГРОЗЫ

Под частотой (вероятностью) реализации угрозы понимаются определенный экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Используются четыре значения этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но применяемые меры существенно затрудняют ее реализацию;

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры обеспечения безопасности ПДн не приняты.

При составлении перечня актуальных угроз ПДн каждому значению показателя ставится в соответствие числовой коэффициент Y2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

РЕАЛИЗАЦИЯ УГРОЗЫ

Коэффициент реализуемости угрозы Y определяется соотношением:

$Y = (Y1 + Y2) / 20$.

По значению коэффициента реализуемости угрозы Y формируется интерпретация реализуемости угрозы:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;
если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;
если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;
если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

ОПРАСНОСТЬ УГРОЗЫ

При оценке опасности угрозы на основе опроса экспертов (специалистов в области защиты информации) определяется показатель опасности угрозы. Этот показатель 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.

ВЫБОР АКТУАЛЬНЫХ УГРОЗ ДЛЯ ИСПДН

Выбор из общего (предварительного) перечня актуальных угроз для ИСПДн осуществляется в соответствии с правилами, приведенными в таблице 2.

Таблица 2 – Правила отнесения угрозы безопасности ПДн к актуальной.

Возможность реализации угрозы (Y)	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

ОБЩИЙ ПЕРЕЧЕНЬ УГРОЗ

Общий перечень угроз и единые исходные данные по ним приведены в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПДН ПО МЕТОДИЧЕСКИМ ДОКУМЕНТАМ ФСТЭК РОССИИ

Состав и содержание угроз определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информационных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

Угрозы классифицируются в соответствии со следующими признаками:

1. **по видам возможных источников угроз:**
   – угрозы, связанные с действиями лиц, имеющих доступ к ИСПДн (внутренний нарушитель);
   – угрозы, связанные с действиями лиц, не имеющих доступ к ИСПДн (внешний нарушитель).
2. **по структуре ИСПДн, на которые направлена реализация угроз:**
   – угрозы в ИСПДн на базе АРМ;

– угрозы в ИСПДн на базе локальных информационных систем;
– угрозы в ИСПДн на базе распределенных информационных систем.

3. по виду несанкционированных действий, осуществляемых с ПДн:

– угрозы, приводящие к нарушению конфиденциальности ПДн (нет непосредственного воздействия на ПДн);
– угрозы, приводящие к несанкционированному воздействию на содержание информации (изменение или уничтожение ПДн);
– угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн (блокирование ПДн).

4. по способам реализации угроз:

– угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования;
– угрозы, реализуемые в ИСПДн при их подключении к сетям международного информационного обмена;
– угрозы, реализуемые в ИСПДн, не имеющих подключений к сетям связи общего пользования и сетям международного информационного обмена.

5. по виду каналов, с использование которых реализуется угроза:

Угрозы, реализуемые по техническим каналам утечки информации

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Источниками угрозы являются физические лица, не имеющие доступа к ИСПДн.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн воспроизводящая ПДн, а так же технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн возможно возникновение угроз за счет реализации следующих технических каналов утечки информации:

– канал утечки акустической (речевой) информации;
– канал утечки видовой информации;
– канал утечки информации за счет ПЭМИН.

1.1.1 Угроза, реализуемая за счет утечки акустической (речевой) информации

Во ИСПДн не осуществляется голосовой ввод ПДн в систему и не используется акустическая система, воспроизводящая ПДн.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

1.1.2 Угроза, реализуемая за счет 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.

Необходимое условие осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Во ИСПДн рабочие места, с которых происходит ввод/редактирование/удаление ПДн, и оборудование, на котором хранятся ПДн, расположены в специальных помещениях с ограниченным доступом. Экраны дисплеев и других средств отображения вычислительной техники операторов расположены специальным образом, исключающим возможность просмотра изображения посторонними лицами. Серверное оборудование не имеет постоянно функционирующих средств отображения информации.

Угрозы утечки видовой информации, связанные с действиями лиц, не имеющих доступ к ИСПДн (внешний нарушитель), маловероятны, так как отсутствует возможность прямой видимости между средством наблюдения и носителем ПДн.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

1.1.3 Угроза, реализуемая за счет утечки информации по каналам ПЭМИН

Угроза утечки информации по каналам ПЭМИН реализуется за счет перехвата техническими средствами побочных (не связанных с прямыми функциональными значениями элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

В данных помещениях функционирует множество ВТСС (телефонные средства; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; средства и системы кондиционирования и т.д.), создающие электромагнитные помехи.

Угрозы утечки информации по каналам ПЭМИН, связанные с действиями лиц, не имеющих доступ к ИСПДн (внешний нарушитель), маловероятны, так как использование данного канала утечки не является эффективным (малое количество ПДн) и очень трудоемким (дорогостоящая специализированная аппаратура, длительное время на настройку и обработку данных). Реализация данной угрозы может привести только к нарушению конфиденциальности части ПДн (копирование, неправомерное распространение).

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

Угрозы, реализуемые за счет несанкционированного доступа к ПДн

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространение), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

– угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

– угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.д.;

– угрозы внедрения вредоносных программ (программно-математического воздействия).

Угрозы, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного программного обеспечения разделяются на Угрозы уничтожения, хищения аппаратных средств ИСПДн путем физического доступа к элементам ИСПДн, а так же на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Источники угрозы НСД в ИСПДн

Источниками угрозы НСД в ИСПДн могут быть:

Нарушители:

1. Нарушители, не имеющие доступ к ИСПДн, реализующие угрозы из внешних сетей общего пользования и (или) сетей международного информационного обмена (внешние нарушители) – к данным нарушителям можно отнести лиц, использующих несанкционированный доступ ИСПДн через сеть общего пользования (Интернет) (существует низкая вероятность подобных действий).

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

– лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступ к ПДн;

– зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места;

– зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам;

– зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн;

– зарегистрированные пользователи ИСПДн с полномочиями системного администратора ИСПДн;

– зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн;

– программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте;

– разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн;

Вредоносные программы:

1. Программные закладки – актуальны, но маловероятны.
2. Программные вирусы – актуальны.
3. Вредоносные программы, распространяющиеся по сети – актуальны.
4. Другие вредоносные программы, предназначенные для осуществления НСД – актуальны.

Аппаратная закладка:

1. Конструктивно встроенная – актуальна, но маловероятна.
2. Автономная – актуальна, но маловероятна.

Уязвимости в ИСПДн

К уязвимостям в ИСПДн относятся:

1. Уязвимости программного обеспечения – актуальны.
2. Уязвимости, вызванные наличием в ИСПДн программно-аппаратной закладки – актуальны, но маловероятны.
3. Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных – актуальны.
4. Уязвимости, вызванные недостатками организации ТЗИ от НСД – актуальны.
5. Уязвимости в СЗИ – актуальны, но маловероятны.
6. Уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств – актуальны.

Объекты воздействия ИСПДн

1. Информация, обрабатывающаяся на АРМ (узле) вычислительной сети:

– на отчужденных носителях информации – дискеты, флэш-накопители и пр.;

– на встроенных носителях долговременного хранения информации – жесткие магнитные диски АРМ и серверов ИСПДн;

– в средствах обработки и хранения информации (ОЗУ, Кэш-память и т.п.) – средства в АРМ и серверах ИСПДн;

– в средствах вывода (портах) ввода/вывода информации – средства в АРМ и серверах ИСПДн.

2. Информация в средствах, реализующих сетевое взаимодействие, и каналах передачи данных – СПД ИСПДн и активное сетевое оборудование.

1.1.4 Угрозы уничтожения, хищения аппаратных средств ИСПДн путем физического доступа к элементам ИСПДн

Кража ПЭВМ

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

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

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

Кража носителей информации

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

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

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – низкая.

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

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

Вывод из строя узлов ПЭВМ и каналов связи

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

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – средняя.

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

Угроза осуществляется путем НСД к информации при проведении ремонта и уничтожения носителей информации, содержащих ПДн.

В Учреждении за техническое обслуживанием узлов ПЭВМ отвечает системный администратор. Перед уничтожением или ремонтом съемных носителей вся информация на них уничтожается.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

Несанкционированное отключение средств защиты

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

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

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – средняя.

1.1.5 Угрозы, реализуемые за счет непосредственного доступа

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода/вывода информации в ИСПДн. Их можно объединить в три группы:

1. Угрозы, реализуемые в ходе загрузки ОС.

2. Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем.
3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.

Угрозы, реализуемые в ходе загрузки ОС

Эти угрозы направлены на перехват паролей и идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехвата управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду АРМ ИСПДн. Чаще всего такие угрозы реализуются с использованием отчужденных носителей информации.

Реализацией данной угрозы могут заниматься внутренние нарушители, то есть зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места, с целью получения доступа к элементам ИСПДн в привилегированном режиме.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – низкая.

Реализация данной угрозы не приводит к негативным последствиям для субъектов персональных данных, т.к. направлена на получение доступа в операционную среду ИСПДн, для нарушения безопасности ПДн необходимо
реализовывать последующие угрозы НСД.

Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем

Эти угрозы направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями ОС или какой-либо прикладной программой общего пользования, так и специально созданными для выполнения несанкционированного доступа программами.

Работа операторов осуществляется на АРМ с использованием специализированного программного обеспечения.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение конфиденциальности ПДн (копирование, неправомерное распространение);
– нарушение доступности (блокирование);
– нарушение целостности (уничтожение, изменение).

Реализация данной угрозы может привести к негативным последствиям для субъектов персональных данных, ущерб может проявляться в виде незапланированных финансовых или материальных затрат.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – средняя.

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ

На АРМ не регламентируется состав используемого программного обеспечения.

Виды нарушений безопасности, в случае реализации угрозы, и непосредственный ущерб совпадают с видами и ущербом для предыдущей угрозы.

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – средняя.

1.1.6 Угрозы, реализуемые за счет удаленного доступа

Угрозы удаленного доступа, реализуемые с использованием протоколов межсетевого взаимодействия:

1. Анализ сетевого трафика.
2. Сканирование сети.
3. Подмена доверенного объекта сети.
4. Навязывание ложного маршрута сети.

5. Внедрение ложного объекта сети.
6. Удаленный запуск приложений.
7. Внедрение по сети вредоносных программ.
8. Угроза выявления пароля.

Анализ сетевого трафика

Угроза реализуется с помощью специальной программы анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передается идентификатор пользователя и его пароль.

Во всех 2-х ИСПДн пользователи не имеют прав на изменение параметров системы и не могут запускать многие приложения, в том числе и программы анализатора пакетов.

Возможные последствия:

Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей.

Реализация данной угрозы не приводит к негативным последствиям для субъектов персональных данных, для нарушения безопасности ПДн необходимо реализовывать последующие угрозы НСД.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – низкая.

Сканирование сети

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них.

В ИСПДн на рабочих станциях, занимающихся обработкой ПДн в ОС отключено максимальное количество неиспользуемых служб. Активное сетевое оборудование ИСПДн настроено так, чтобы закрыть все неиспользуемые порты.

Возможные последствия:

Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Реализация данной угрозы не приводит к негативным последствиям для субъектов персональных данных, для нарушения безопасности ПДн необходимо реализовывать последующие угрозы НСД.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Подмена 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.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

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.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

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, 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.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

Удаленный запуск 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 документа, 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, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Внедрение 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.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Угроза выявления пароля

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Реализуется с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена объекта сети (IP-spoofing) и перехват пакетов (sniffing).

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Возможные последствия:

Выполнение любого действия, связанного с получением несанкционированного доступа.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение конфиденциальности ПДн (копирование, неправомерное распространение);

– нарушение доступности (блокирование);

– нарушение целостности (уничтожение, изменение).

Реализация данной угрозы может привести к негативным последствиям для субъектов персональных данных, непосредственный ущерб может проявляться в виде незапланированных финансовых или материальных затрат.

1.1.7 Отказ в обслуживании

Угроза основана на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда ОС оказывается не в состоянии обрабатывать поступающие пакеты.

Разновидности угроз «Отказ в обслуживании»:

Скрытый отказ в обслуживании, вызванный частичным исчерпанием ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов.

Возможные последствия:

Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов персональных данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

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.

Возможные последствия:

Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов персональных данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

Явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации.

Возможные последствия:

Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов и т.п.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов персональных данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

Явный отказ в обслуживании, вызванный использованием ошибок в ПО. Передача 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.

Возможные последствия:

Нарушение работоспособности сетевых устройств.

Частота (вероятность) реализации угрозы – маловероятная (Y_2=0).

Опасность угрозы – низкая.

Виды нарушений безопасности в случае реализации угрозы:

– нарушение доступности (блокирование).

Реализация данной угрозы может привести к незначительным негативным последствиям для субъектов персональных данных. Непосредственный ущерб может проявляться в виде незапланированных временных затрат субъекта.

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

1.2.1 Действия вредоносных программ

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 Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения. Осуществляется ежедневное обновление антивирусных средств и антивирусных баз.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

1.2.2 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.

В Учреждении введено разграничение прав пользователей на установку ПО и осуществляется контроль. Пользователи проинструктированы о порядке установки ПО.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера

1.3.1 Утрата ключей и атрибутов доступа

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

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

1.3.2 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 Учреждении не осуществляется резервное копирование обрабатываемых ПДн.

Частота (вероятность) реализации угрозы – средняя (Y_2=5).

Опасность угрозы – средняя.

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

Частота (вероятность) реализации угрозы – низкая (Y2=2).

Опасность угрозы – средняя.

1.3.4 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 Учреждении не осуществляет резервирование ключевых элементов ИСПДн.

Частота (вероятность) реализации угрозы – средняя (Y_2=5).

Опасность угрозы – средняя.

1.3.5 Сбой системы электроснабжения

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

В Учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

1.3.6 Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

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

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – низкая.

Угрозы преднамеренных действий пользователей, угрозы неантропогенного и стихийного характера

1.4.1 Доступ к информации, ее модификация и уничтожение лицами, не допущенными 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 Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых этажах здания.

Частота (вероятность) реализации угрозы – маловероятная (Y2=0).

Опасность угрозы – низкая.

1.4.2 Разглашение информации, ее модификация и 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 Учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Договор об их неразглашении.

Частота (вероятность) реализации угрозы – низкая (Y_2=2).

Опасность угрозы – средняя.

Таблица 1 – Перечень угроз для ИСПДн «ПараГраф: Район»

Наименование Угрозы (ИСПДн имеет низкий уровень исходной защищенности (Y_1=5))		Частота (вероятность) реализации угрозы, Y_2	Возможность реализации угрозы, Y	Опасность угрозы	Актуальность
Угрозы, реализуемые через технические каналы утечки информации					
1.	Угроза утечки акустической (речевой) информации	Маловероятная (Y_2=0)	Низкая (Y=0,25)	Низкая	Неактуальная
2.	Угрозы утечки видовой информации	Маловероятная (Y_2=0)	Низкая (Y=0,25)	Низкая	Неактуальная
3.	Угрозы утечки информации по каналам ПЭМИН	Маловероятная (Y_2=0)	Низкая (Y=0,25)	Низкая	Неактуальная
Угрозы, реализуемые за счет несанкционированного доступа к ПДн					
4.	Угрозы уничтожения, хищения аппаратных средств ИСПДн путем физического доступа к элементам ИСПДн				
4.1.	Кража ПЭВМ	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
4.2.	Кража носителей информации	Низкая (Y_2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
4.3.	Кража, модификация, уничтожение информации	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
4.4.	Вывод из строя узлов ПЭВМ, каналов связи	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
4.5.	Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
4.6.	Несанкционированное отключение средств защиты	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
5	Угрозы непосредственного доступа				
5.1.	Угрозы, реализуемые в ходе загрузки ОС	Низкая (Y_2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
5.2.	Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
5.3.	Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
6.	Угрозы удаленного доступа				
6.1.	Анализ сетевого трафика	Низкая (Y_2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
6.2.	Сканирование сети	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
6.3	Подмена доверенного объекта сети	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
6.4	Навязывание ложного маршрута сети	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная

6.5	Внедрение ложного объекта сети	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
6.6	Удаленный запуск приложений	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
6.7	Внедрение по сети вредоносных программ	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
6.8	Угроза выявления пароля	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
7	Отказ в обслуживании				
7.1	Скрытый отказ в обслуживании (частичное исчерпание ресурсов)	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
7.2	Явный отказ в обслуживании (исчерпание ресурсов)	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
7.3	Явный отказ в обслуживании (нарушение логической связности)	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
7.4	Явный отказ в обслуживании (ошибки в ПО)	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).					
8.	Действия вредоносных программ (вирусов)	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
9.	Установка ПО, не связанного с исполнением служебных обязанностей	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.					
10.	Утрата ключей и атрибутов доступа	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
11.	Непреднамеренная модификация (уничтожение) информации сотрудниками	Средняя (Y_2=5)	Средняя (Y=0,5)	Средняя	Актуальная
12.	Непреднамеренное отключение средств защиты	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная
13.	Выход из строя аппаратно-программных средств	Средняя (Y_2=5)	Средняя (Y=0,5)	Средняя	Актуальная
14.	Сбой системы электроснабжения	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
15.	Стихийное бедствие	Низкая (Y_2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
Угрозы преднамеренных действий пользователей, угрозы неантропогенного и стихийного характера					
16.	Доступ к информации, ее модификация и уничтожение лицами, не допущенными к ее обработке	Маловероятная (Y_2=0)	Средняя (Y=0,25)	Низкая	Неактуальная
17.	Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к ее обработке	Низкая (Y_2=2)	Средняя (Y=0,35)	Средняя	Актуальная

Состав программных и технических средств защиты информации для создания и эксплуатации системы защиты информации в ИСПДн приведен ниже:

Перечень предлагаемых технических средств представлен в таблице 2.

Таблица 2 – Перечень предлагаемых технических средств

Подсистемы и требования	Применяемое СрЗИ (выполнение требования)
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
- в операционную систему	eToken (Etoken PKI Client и eToken Network Logon); СрЗИ Dallas Lock; Встроенные средства ОС
2. Подсистема регистрации и учета	
2.1. Учет носителей информации	Журнал учета носителей;
3. Подсистема обеспечения целостности	
3.1. Обеспечение целостности программных средств и обрабатываемой информации	eToken; СрЗИ Dallas Lock:
3.2. Физическая охрана ИСПДн	Пропускной режим
3.3. Периодическое тестирование СрЗИ НСД	eToken; СрЗИ Dallas Lock;
3.4 Наличие средств восстановления СрЗИ НСД	Резервные копии
4. Подсистема антивирусной защиты	Dr. Web Security Space
5. Подсистема обеспечения безопасного межсетевого взаимодействия	СЗИ “Застава”
6. Подсистема обнаружения вторжений	Dr. Web Security Space

Применяемые для нейтрализация актуальных угроз СрЗИ представлены в таблице 3.

Таблица 3 – Нейтрализация актуальных угроз

Наименование Угрозы		Применяемое СрЗИ (нейтрализация угрозы)
Угрозы, реализуемые за счет несанкционированного доступа		
1.	Вывод из строя узлов ПЭВМ, каналов связи	Организационные меры
2.	Несанкционированное отключение СрЗИ	Организационные меры; eToken; СрЗИ Dallas Lock; Встроенные средства ОС Dr. Web Security Space 12
3.Угрозы доступа (проникновения) в операционную среду		
3.1.	Угрозы, реализуемые после загрузки ОС независимо от того, какая прикладная программа запускается пользователем	Организационные меры; eToken; СрЗИ Dallas Lock; Встроенные средства ОС Dr. Web Security Space 12
3.2.	Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ	Организационные меры; eToken; СрЗИ Dallas Lock; Встроенные средства ОС Dr. Web Security Space 12

4.Угрозы удаленного доступа		
4.1.	Анализ сетевого трафика	СЗИ “Застава” Dr. Web Security Space 12
42.	Сканирование сети	СЗИ “Застава” Dr. Web Security Space 12
4.3.	Выявление пароля	СЗИ “Застава” Dr. Web Security Space 12
4.4.	Удаленный запуск приложений	СЗИ “Застава” Dr. Web Security Space 12
4.5.	Внедрение по сети вредоносных программ	eToken; СрЗИ Dallas Lock; Встроенные средства ОС; СЗИ “Застава” Dr. Web Security Space 12
5. Угрозы хищения, несанкционированной модификации или блокирования информации с применением ПМВ		
5.1.	Действия вредоносных программ (вирусов)	Dr. Web Security Space 12
5.2	Установка ПО, несвязанного с исполнением служебных обязанностей	Организационные меры
6. Угрозы непреднамеренных действий пользователей и стихийного характера		
6.1.	Непреднамеренное отключение средств защиты	Организационные меры применение СрЗИ
6.2.	Выход из строя аппаратно-программных средств	Применение средств тестирования СрЗИ
7. Угрозы преднамеренных действий пользователей		
7.1.	Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к ее обработке	Организационные меры; Применение СрЗИ