ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КРЫМ «САКСКИЙ ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»
ОКПО 00777480, ОГРН 1149102125963, ИНН 9107003995, КПП 910701001
Ул. Заводская,52, г. Саки, Республика Крым, 296500
Тел. (36563) 2-83-08 E-mail: 036@crimeaedu.ru

УТВЕРЖДАЮ
Директор ГБПОУ РК «Сакский технологический техникум»

Н.Н. Наседкин
15.05.2023г.

Модель угроз безопасности персональных данных

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.

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

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

Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн ГБПОУ РК «Сакский технологический техникум» строится на основании следующих документов:

- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;
- Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах 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.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

- Анализ УБПДн включает:
- Описание угроз.
- Оценку вероятности возникновения угроз.
- Оценку реализуемости угроз.
- Оценку опасности угроз.
- Определение актуальности угроз.

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

1.Описание ИСПДн

ИСПДн позволяет осуществлять сбор, хранение, использование и уничтожение персональных данных, содержащих информацию, позволяющую получить дополнительную информацию о субъекте персональных данных.

1.1 Состав ПО ИСПДн

Для данной ИСПДн в целом необходимо обеспечить следующие характеристики безопасности информации – конфиденциальность, целостность.

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

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного воздействия.

2. Пользователи

В ГБПОУ РК «Сакский технологический техникум» обработка персональных данных осуществляется 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.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 1.

Таблица 1 – Матрица доступа

Группа	*Уровень доступа к ПДн*	*Разрешенные действия*
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	сбор систематизация накопление хранение уточнение использование уничтожение
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	сбор систематизация накопление хранение уточнение использование уничтожение
Операторы ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	сбор систематизация накопление хранение уточнение использование уничтожение использование

Предоставление или прекращение доступа к ИСПДн осуществляется в соответствии с приказом о назначении на должность или приказом об увольнении.

3. Тип ИСПДн

Таблица 2 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	*Типовая информационная система*
Структура информационной системы	Локальная информационная система
Подключение информационной системы к сетям общего пользования и (или)	Имеется

сетям международного информационного обмена	
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	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 (или) доступности

ЛИС II типа – локальная информационная система, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

4. Исходный уровень защищенности ИСПДн

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

В таблице представлены характеристики уровня исходной защищенности для ИСПДн ГБПОУ РК «Сакский технологический техникум».

Таблица 3 – Исходный уровень защищенности

Позиция	*Технические и эксплуатационные характеристики*	*Уровень защищенности*
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	Высокий

Определение исходной степени защищенности:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70 % характеристик соответствуют уровню «высокий»;

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПДн соответствуют уровню не ниже «средний»;

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Таблица 4

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	3	42%
2	Средний	2	29%
3	Низкий	2	29%

В соответствии с полученными данными устанавливается **средний показатель исходной защищенности**, значение коэффициента $\mathbf{Y_1=5}$.

5. Вероятность реализации угроз безопасности

5.1 Классификация угроз безопасности

Перечень угроз, уязвимостей и технических каналов утечки информации сформирован в соответствии с требованиями руководящих документов ФСТЭК России.

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

ИСПДн Учреждения представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными элементами ИСПДн являются:

- персональные данные, обрабатываемые в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации (СЗИ), включая СКЗИ;
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
- документация на СКЗИ и на технические и программные компоненты ИСПДн;
- ключевая, аутентифицирующая и парольная информация;
- помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающиеУБПДн;

- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

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

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;

- носитель вредоносной программы.

5.2 Классификация нарушителей

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

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

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

Внешний нарушитель

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

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

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

Внутренний нарушитель

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

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

администраторы ИСПДн (категория I);

администраторы конкретных подсистем или баз данных ИСПДн (категория II);

пользователи ИСПДн (категория III);

пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);

лица, обладающие возможностью доступа к системе передачи данных (категория V);

сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);

обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.) (категория VII);

уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

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

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

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

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

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

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

общая информация – информации о назначения и общих характеристиках ИСПДн;

эксплуатационная информация – информация, полученная из эксплуатационной документации;

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

В частности, нарушитель может иметь:

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

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

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

данные о реализованных в ПСЗИ принципах и алгоритмах;

исходные тексты программного обеспечения ИСПДн;

сведения о возможных каналах реализации угроз;

информацию о способах реализации угроз.

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

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

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

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

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

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

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

Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

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

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи;
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

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

5.3 Классификация уязвимостей ИСПДн

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 персональных данным.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

5.4 Перечень возможныхУБПДн

Для ИСПДн Учреждения можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам.

1.1. Угрозы утечки акустической информации.

1.2. Угрозы утечки видовой информации.

1.3. Угрозы утечки информации по каналам ПЭМИН.

2. Угрозы несанкционированного доступа к информации.

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

2.1.1. Кража ПЭВМ;

2.1.2. Кража носителей информации;

2.1.3. Кража ключей и атрибутов доступа;

2.1.4. Кражи, модификации, уничтожения информации;

2.1.5. Вывод из строя узлов ПЭВМ, каналов связи;

2.1.6. Несанкционированное отключение средств защиты.

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);

2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных;

2.2.3. Установка ПО не связанного с исполнением служебных обязанностей.

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;

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками;

2.3.3. Непреднамеренное отключение средств защиты;

2.3.4. Выход из строя аппаратно-программных средств;

2.3.5. Сбой системы электроснабжения;

2.3.6. Стихийное бедствие.

2.4. Угрозы преднамеренных действий внутренних нарушителей.

2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

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;

2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;

2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.

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.

2.5.3. Угрозы выявления паролей по сети.

2.5.4. Угрозы навязывание ложного маршрута сети.

2.5.5. Угрозы подмены доверенного объекта в сети.

2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

2.5.7. Угрозы типа «Отказ в обслуживании».

2.5.8. Угрозы удаленного запуска приложений.

2.5.9. Угрозы внедрения по сети вредоносных программ.

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).

5.5.1 Угрозы утечки информации по техническим каналам

5.5.1.1 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.

5.5.1.2 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.

На окнах используются жалюзи и занавески. Доступ посторонних лиц в помещения, в которых производится обработка ПДН, ограничен.

Вероятность реализации угрозы – маловероятна.

5.5.1.3 Угрозы утечки информации по каналам ПЭМИН.

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

Угроза утечки информации, содержащей ПДн, по каналу ПЭМИН возможна, за счет перехвата техническими средствами разведки за пределами контролируемой зоны ПЭМИН, возникающих при обработке ПДн средствами вычислительной техники ИСПДн. Наиболее опасным режимом работы средств вычислительной техники является вывод

информации на экран монитора автоматизированного рабочего места оператора (пользователя) ИСПДн.

Элементы ИСПДн находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется с множеством других паразитных сигналов элементов не входящих в ИСПДн.

Вероятность реализации угрозы – маловероятна.

5.5.2. 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).

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

Кража ПЭВМ.

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

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации. В результате возможно несанкционированное копирование разделов системы хранения данных штатными средствами на съемные устройства хранения.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.Хранение носителей осуществляется в сейфе.

Доступ к техническим средствам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора. Переносные компьютеры для обработки ПДН в ИСПДН не используются.

Вероятность реализации угрозы – маловероятна.

Кража ключей и атрибутов доступа.

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

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

Кражи, модификации, уничтожения информации

Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

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. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

Несанкционированное отключение средств защиты.

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

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Возможность отключения или изменения настроек СЗИ пользователем запрещена. Настройка средств разграничения доступа к ресурсам ИСПДн производится системным администратором.

Вероятность реализации угрозы – маловероятна.

5.5.2.2 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).

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

Вероятность реализации угрозы – является низкой.

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 повышается:

- при увеличении элементов, в том числе программного обеспечения, ИСПДн;
- при увеличении числа функциональных связей между элементами;
- наличии подключения к сетям общего доступа и (или) международного обмена.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 5.

Таблица 5

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	низкая	2
Распределенная ИС II типа	низкая	2

В случае если в обработке персональных данных участвует ПО собственной разработки или стандартное ПО, доработанное под нужды учреждения, то следует повысить значение вероятности реализации угрозы:

- для всех типов ИСПДн, кроме Автономная ИС I типа, на порядок;
- для Распределенной ИС II типа на два порядка.

В данном случае рассматривается Локальная ИС II типа.

Вероятность реализации угрозы – **является низкой**.

Установка ПО не связанного с исполнением служебных обязанностей

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

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

Вероятность реализации угрозы –**маловероятна**.

5.5.2.3 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.

Утрата ключей и атрибутов доступа.

Угроза может осуществляться за счет 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 сложность пароля и периодическую его смену, введена политика «чистого стола». Пользователи проинструктированы о парольной политике и о действиях в случае утраты или компрометации паролей.

Вероятность реализации угрозы – **является низкой.**

Непреднамеренная модификация (уничтожение) информации сотрудником.

Угроза может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают правила работы с конфиденциальной информацией.

Перед началом работы каждый пользователь изучает Инструкцию пользователя. В Учреждении осуществляется резервное копирование обрабатываемыхПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятна.**

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,

Вероятность реализации угрозы - **маловероятна**.

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 Учрежденииосуществляется резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

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 и осуществляется резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

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

Вероятность реализации угрозы – **маловероятна**.

5.5.2.4 Угрозы преднамеренных действий внутренних нарушителей

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

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

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

Вероятность реализации угрозы – **маловероятна**.

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 Учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Вероятность реализации угрозы – **является низкой**.

5.5.2.5 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.

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.

Перехват за переделами контролируемой зоны.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 6.

Таблица 6

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

В нашем случае, предполагается Локальная ИС II типа.

Вероятность реализации угрозы – **является низкой.**

Перехват в пределах контролируемой зоны внешними нарушителями

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

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок

Вероятность реализации угрозы – **маловероятна**.

Угроза «Сканирование сети» в локальной 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. Реализация данной угрозы в локальной сети наиболее вероятна со стороны внутреннего нарушителя.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 7.

Таблица 7

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0

Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

В нашем случае имеем: Локальная ИС II типа.

Вероятность реализации угрозы – **маловероятна.**

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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 8.

Таблица 8

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **низкая вероятность.**

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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 9.

Таблица 9

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **маловероятна.**

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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 10.

Таблица 10

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **маловероятна.**

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 NovellNetWare; 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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 11.

Таблица 11

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0

ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

В нашем случаеЛокальная ИС II типа.

Вероятность реализации угрозы – **маловероятна..**

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 (Pingflooding), 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 RedirectHost, 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 «PingDeath»), 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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 12.

Таблица 12

Тип ИСПДн	*Вероятность реализации угрозы*	*Коэфф. вероятности реализации угрозы нарушителем*
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	низкая	2
Распределенная ИС II типа	низкая	2

Серверы ИСПДн, а также сегмент ИСПДн в учреждении защищены межсетевым экраном. В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **низкая вероятность**.

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, 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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 13.

Таблица 13

Тип ИСПДн	Вероятность реализации угрозы	Коэфф. вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **низкая вероятность.**

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.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – **является маловероятной**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 14.

Таблица 14

Тип ИСПДн	Вероятность реализации угрозы	Коэфф. вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0

Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – **низкая вероятность.**

6. Реализуемость угроз

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$

Оценка реализуемости УБПДн представлена в таблице.

Таблица 15 – 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. Несанкционированное отключение средств защиты	0,25	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,35	средняя

2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,25	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	0,35	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,25	низкая
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая
2.3.4. Выход из строя аппаратно-программных средств	0,25	низкая
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	0,35	средняя
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:		
2.5.1.1. Перехват за пределами с контролируемой зоны	0,35	средняя
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.	0,25	низкая
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	0,35	средняя

обслуживании»		
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя

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 16 – Опасность УБПДн

Тип угроз безопасности ПДн	*Опасность угрозы*
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая
1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	низкая
2.1.2. Кража носителей информации	низкая
2.1.3. Кража ключей и атрибутов доступа	низкая
2.1.4. Кражи, модификации, уничтожения информации	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	низкая
2.1.6. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	средняя
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	средняя
2.3.2. Непреднамеренная модификация (уничтожение)	низкая

информации сотрудниками	
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:	
2.5.1.1. Перехват за пределами 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	средняя
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	средняя

8. Определение актуальности угроз в ИСПДн

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

Таблица 17 – 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 18 – Актуальность УБПДн

Тип угроз безопасности ПДн	*Опасность угрозы*
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	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	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	неактуальная
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 пределами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними	неактуальная

нарушителями.	
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	актуальная

Были выявлены следующие актуальные угрозы:

- действия вредоносных программ (вирусов)
- утрата ключей и атрибутов доступа
- угрозы внедрения по сети вредоносных программ

Для снижения опасности реализации актуальных УБПДн рекомендуется:

- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.
- постоянное обновление антивирусных баз.