Министерство здравоохранения и социального развития
Российской Федерации

СОГЛАСОВАНО

Начальник 2 управления
ФСТЭК России

_____ А.В. Куц

«22» декабря 2009 г.

УТВЕРЖДАЮ

Директор Департамента
информатизации Министерства
здравоохранения и социального
развития Российской Федерации

_____ О.В. Симаков

«23» декабря 2009 г.

Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости

Москва 2009

СОДЕРЖАНИЕ

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

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

Настоящие Методические рекомендации по составлению Частной модели угроз безопасности персональных данных (далее – Методические рекомендации) при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости (далее – Учреждения) с использованием средств автоматизации, разработаны в соответствии с п. 12 постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Методические рекомендации содержат систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Методические рекомендации являются методическим документом и предназначены для операторов персональных данных Учреждений, осуществляющих обработку ПДн, и используются при решении следующих задач:

- разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

- контроль за обеспечением уровня защищенности 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 информацион-

ной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

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

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

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

1 Общие положения

Работы по созданию Частной модели угроз безопасности персональных данных, при их обработке в информационных системах персональных данных с использованием средств автоматизации (далее – информационная система) проводятся в соответствии со следующими основными документами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее – Положение);

- Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462) (далее – Порядок);

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

В соответствии с п. 2 Положения безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки инфор-

мации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

В соответствии с п. 12 Положения необходимым условием разработки системы защиты персональных данных является формирование модели угроз безопасности персональных данных (далее – модель угроз).

Кроме этого, в соответствии с п. 16 Порядка модель угроз необходима для определения класса специальной информационной системы.

Модель угроз формируется и утверждается оператором в соответствии с методическими документами, разработанными в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Модель угроз может быть пересмотрена:

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

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

2 Методология формирования модели угроз

Разработка модели угроз должна базироваться на следующих принципах:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн).

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗПДн не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

Для разработки модели угроз необходимо последовательно осуществить следующие шаги:

1) описать ИСПДн (см. раздел 3 на стр. 19);

2) определить пользователей ИСПДн (см. раздел 4 на стр. 25);

3) определить тип ИСПДн (см. раздел 5 на стр. 28);

4) определить исходный уровень защищенности ИСПДн (см. раздел 6 на стр. 32);

5) определить вероятность реализации угроз в ИСПДн (см. раздел 7 на стр. 36);

6) определить возможность реализации угроз в ИСПДн (см. раздел 8 на стр. 71);

7) оценить опасность угроз (см. раздел 9 на стр. 90);

8) определить актуальность угроз в ИСПДн (см. раздел 10 на стр. 104);

После прохождения всех шагов будет сформирована частная модель угроз. Модель угроз составляется для каждой выявленной ИСПДн и оформляется в виде документа Модель угроз безопасности персональных данных.

3 Описание ИСПДн

Описание ИСПДн является первым шагом при построении модели угроз и осуществляется на этапе сбора и анализа исходных данных.

Описание ИСПДн состоит из следующих пунктов:

1) Описание условий создания и использования ПДн;

2) Описание форм представления ПДн;

3) Описание структуры ИСПДн;

4) Описание характеристик безопасности.

3.1 Определение условий создания и использования персональных данных

Должны быть описаны условия создания и использования персональных данных. Для этого определяются характер и структура обрабатываемых персональных данных:

- цель обработки ПДн;

- состав ПДн (фамилия, имя, отчество, дата рождения, паспортные данные, сведения о состоянии здоровья (перечислить) и т.п.);

- действия осуществляемые с данными в ходе их обработки (действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных);

- условия прекращения обработки;

- субъекты, создающие персональные данные (в качестве такого субъекта может выступать лицо или его представитель в виде программного или технического средства);

- субъекты, которым персональные данные предназначены;

- правила доступа к защищаемой информации;

- информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных;

- используемые в процессе создания и использования персональных данных объекты, которые могут быть объектами угроз, создающими условия для появления угроз персональным данным. Такого рода объектами могут быть, например, технические и программные средства.

Определение условий создания и использования ПДн осуществляется на основании Отчета о результатах проведения внутренней проверки.

3.2 Описание форм представления персональных данных

Персональные данные имеют различные формы представления (носители ПДн) с учетом используемых в информационной системе информационных технологий и технических средств.

Носитель ПДн – 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.

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимой акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

- видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.

Необходимо дать описание носителей персональных данных.

Основными носителями ПДн в ИСПДн Учреждений являются:

- видовая информация;

- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.

Остальные типы носителей можно исключить по следующим причинам:

- акустическую (речевую) информацию, если в ИСПДн не производится голосового ввода персональных данных;

- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов, если все элементы ИСПДн находятся внутри контролируемой зоны.

Формы представления и носители ПДн определятся на основании Отчета о результатах проведения внутренней проверки.

3.3 Описание структуры ИСПДн

На основе анализа условий создания и использования персональных данных должны быть определены элементы и информация, сопутствующая процессам создания и использования персональных данных.

После этого должна быть описана структура и представлена схеме ИСПДн, а так же описаны элементы ИСПДн:

1) Технические средства ИСПДн, в том числе:

- Описание серверов баз данных, где хранятся ПДн. Если сервера БД имеют уникальную программную, техническую или логическую структуру, необходимо описание каждого сервера.

- Описание серверов БД, расположенных вне пределов контролируемой зоны или являющихся частью других ИСПДн, с которыми ваша информационная система обменивается данными.

- Описание АРМ пользователей. Если в вашей информационной системе АРМ пользователей унифицированы, то достаточно перечислить программное обеспечение используемое, при обработке ПДн и установленные средства безопасности.

2) Используемые каналы связи, с помощью которых ИСПДн обменивается данными с другими системами. Каналом связи так же является подключение всей ИСПДн или ее элементов к сети международного обмена Интернет, даже если режим работы информационной системы не предполагает служебной необходимости передачи данных по сетям общего пользования и международного обмена.

Описание канала производится в форме:

- Характеристика канала (выделенный канал, модемное подключение и т.п.);

- Получатели данных (орган исполнительной власти (название), контролирующие органы (название) и т.п.);

- Характер и вид пересылаемых данных (консолидированные отчеты, синхронизация данных между БД и т.п.).

3) Программные средства ИСДН, в их числе:

- Используемые операционные системы;

- Используемые программно-аппаратные комплексы, участвующие в обработке ПДн;

- Основное пользовательское программное обеспечение, участвующие в обработке ПДн;

- ПО собственной разработки или стандартные программы, специально доработанные под нужды организации;

- Антивирусную защиту.

4) Циркулирующие в ИСПДн информационные потоки, в виде:

отправитель (физическое или юридическое лицо, процесс, программный модуль и т.п.) – получатель (физическое или юридическое лицо, процесс,

программный модуль и т.п.): формат обмена данными (ежемесячные (квартальные) отчеты, регистры, реестры, запросы абонентов и т.п.).

5) Описать используемые технические средства и принципы защиты, отобразить их на общей схеме ИСПДн. Могут включать в себя:

- Межсетевые экраны;
- Граничное телекоммуникационное оборудование;
- Оборудование формирующие виртуальные частные сети (VPN);
- Разделение на виртуальные локальные сети (VLAN, Virtual Local Area Network).

Структура ИСПДн определяется на основании Отчета о результатах проведения внутренней проверки.

3.4 Определение характеристик безопасности

Так же необходимо определить характеристики безопасности элементов системы и всей ИСПДн в целом.

Основными (классическими) характеристиками безопасности являются конфиденциальность, целостность и доступность.

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

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

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

При обработке персональных данных в ИСПДн учреждений Минздравсоцразвития России необходимо обеспечить следующие характеристики безопасности – конфиденциальность, целостность.

Выбранные характеристики безопасности ПДн отражаются в Акте классификации информационной системы персональных данных.

4 Пользователи ИСПДн

В данном разделе вам необходимо составить матрицу доступа. Матрица доступа в табличной форме отражает права всех групп пользователей ИСПДн на действия с персональными данными. Действия (операции) с персональными данными, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

Есть три основные группы пользователей ИСПДн (группы описаны в Концепции информационной безопасности):

- Администраторы ИСПДн, осуществляющие настройку и установку технических средств ИСПДн и обеспечивающие ее бесперебойную работу;

- Разработчики ИСПДн, осуществляющие разработку и поддержку программного обеспечения собственной разработки или стандартных программ, специально доработанных под нужды организации;

- Операторы ИСПДн, осуществляющие текущую работу с персональными данными.

Каждая группа может быть уточнена (пример уточнения описан в Политике информационной безопасности), например, может быть две группы Операторов ИСПДн. Первая осуществляет лишь сбор и систематизацию персональных данных, вторая – уточнение, использование и распространение. В матрице доступа должно быть описание всех групп, обладающих правами на определенные действия с ПДн. Должен быть уточнен список разрешенных действий каждой из групп.

Типовая матрица доступа для ИСПДн учреждений Минздравсоцразвития России представлена в таблице 1.

Таблица 1

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.	- сбор - систематизация - накопление - хранение

	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.	- уточнение - использование - распространение - обезличивание - блокирование - уничтожение
Разработчик ИСПДн	Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информацией о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн	- систематизация - накопление - хранение - уточнение - обезличивание - блокирование - уничтожение
Оператор ИСПДн	Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - распространение - обезличивание

Должен быть описан порядок предоставления и прекращения доступа тем или иным пользователям. При наступлении, каких событий (прием и увольнение с работы, инициатива или требование руководителя, службы безопасности и т.п.) и на основании каких документов (политик и инструкций) происходит предоставление и прекращение доступа.

Впоследствии сотрудники выявленных групп пользователей, должны быть рассмотрены в качестве потенциальных нарушителей (см. раздел 7.2 на стр. 37).

5 Типы ИСПДн

Угрозы безопасности персональных данных (УБПДн) зависят от типа ИСПДн. ИСПДн различают по следующим характеристикам.

5.1 Характеристики ИСПДн

По структуре информационные системы подразделяются:

- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

- на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

ИСПДн имеет подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, если вся система или ее элементы пересылают данные по электронным каналам связи в другие системы или имеют подключение к сети Интернет.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

ИСПДн является однопользовательской, когда один сотрудник сочетает в себе роли Администратора и Пользователя ИСПДн, и единолично осуществля-

ет обработку персональных данных на одном автоматизированном рабочем месте. Во всех других случаях, ИСПДн является многопользовательской.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

ИСПДн является системой с разграничением прав, если в ней присутствуют разные группы пользователей с разными правами (см. раздел 4 на стр. 25). ИСПДн является системой без разграничения прав, когда все пользователи имеют одинаковые права на действия с персональными данными.

Информационные системы **в зависимости от местонахождения** их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

Все ИСПДн Минздравсоцразвития России, находятся пределах Российской Федерации. Если какие-либо элементы ИСПДн находятся вне пределов Российской Федерации, то ИСПДн рассматривается, как Распределенная ИС II типа (см. раздел 5.2 на стр. 29) с соответствующими УБПДн.

5.2 Типизация ИСПДн

Исходя из характеристик ИСПДн (см. раздел 6.1.), определяется тип ИСПДн Учреждений. Существуют следующие типы ИСПДн:

- **Автономная ИС I типа –** однопользовательское, автономное рабочее место, не имеющее подключения к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы.

- **Автономная ИС II типа –** однопользовательское, автономное рабочее место, имеющее подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы.

- **Автономная ИС III типа –** многопользовательское автономное рабочее место, не имеющее подключения к сетям связи общего пользования и (или) се-

тям международного информационного обмена информационные системы, без разграничения прав доступа.

- **Автономная ИС IV типа –** многопользовательское, автономное рабочее место, имеющее подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, без разграничения прав доступа.

- **Автономная ИС V типа –** многопользовательское, автономное рабочее место, не имеющее подключения к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

- **Автономная ИС VI типа –** многопользовательское, автономное рабочее место, имеющее подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

- **ЛИС I типа –** локальная информационная система, не имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

- **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.

- **Распределенная ИС I типа –** распределенная информационная система, не имеющая подключения к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

- **Распределенная ИС II типа –** распределенная информационная система, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

Необходимо определить к какому типу относится ИСПДн. После чего, в соответствии с типом ИСПДн, определить уровень исходной защищенности (см. раздел 6 на стр. 32), вероятность (см. раздел 7 на стр. 36) и возможность реализации угроз (см. раздел 8 на стр. 71), их опасность (см. раздел 9 на стр. 90) и актуальность (см. раздел 10 на стр. 104).

В приложении представлены обобщенные частные модели угроз для каждого из типов ИСПДн (см. Приложения на стр. 124).

Данная типизация введена для упрощения построения модели угроз и используется лишь в данной Методике. Данные типы **не должны** использоваться при составлении в Актах классификации ИСПДн и любых других документов.

6 Уровень исходной защищенности

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1), приведенных в таблице 2.

Таблица 2

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;		+	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;		+	
локальная ИСПДн, развернутая в пределах одного здания.	+		
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;		+	
ИСПДн, физически отделенная от сети общего пользования.	+		
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+		
запись, удаление, сортировка;		+	
модификация, передача.			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем			+

ИСПДн;			
ИСПДн с открытым доступом.			+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн.	+		
6. По уровню (обезличивания) ПДн:			
ИСПДн в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+		
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
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 всю БД с ПДн;			+
ИСПДн, предоставляющая часть ПДн;		+	
ИСПДн, не предоставляющие никакой информации.	+		

Исходная степень защищенности определяется следующим образом:

1) ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу) ($Y_1 = 0$).

2) ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответ-

ствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности (Y_1= 5).

3) ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 (Y_1= 10).

Уровень исходной защищенности должен быть определен для каждой ИСПДн.

Особое внимание следует уделить определению Наличия соединения с другими базами ПДн в иных ИСПДн (пункт 5, таблицы 2) и Объему ПДн, предоставляемых сторонним пользователям ИСПДн без предварительной обработки (пункт 7, таблицы 2).

Для Распределенных ИС обоих типов, важно определить их территориальное размещение (пункт 1, таблицы 2).

В таблице 3 представлено обобщенное определение уровня исходной защищенности для каждого из типов ИСПДн.

Таблица 3

Технические и эксплуатационные характеристики	Автономная ИС I типа	Автономная ИС II типа	Автономная ИС III типа	Автономная ИС IV типа	Автономная ИС V типа	Автономная ИС VI типа	ЛИС I типа	ЛИС II типа	Распред. ИС I типа	Распред. ИС II типа
По территориальному размещению	высокий	высокий	высокий	высокий	высокий	высокий	высокий	высокий	средний	средний
По наличию соединения с сетями общего пользования	высокий	средний	высокий	средний	высокий	средний	высокий	средний	средний	средний
По встроенным (легальным) операциям с записями баз персональных данных	средний	средний	средний	средний	средний	средний	средний	средний	низкий	низкий
По разграничению доступа к персональным данным	средний	средний	средний	средний	средний	средний	средний	средний	средний	средний
По наличию соединений с другими базами ПДн иных ИСПДн	высокий	высокий	высокий	высокий	высокий	высокий	высокий	высокий	высокий	высокий
По уровню (обезличивания) ПДн	средний	средний	средний	средний	средний	средний	средний	средний	средний	средний
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний	средний	средний	средний	средний	средний	средний	средний	средний	средний
Уровень защищенности	средний	средний	средний	средний	средний	средний	средний	средний	средний	средний
Значение Y_1	5	5	5	5	5	5	5	5	5	5

Определение исходного уровня защищенности определяется на основании Отчета о результатах проведения внутренней проверки.

7 Вероятность реализации угроз безопасности

7.1 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 учреждений и организаций Минздравсоцразвития России представляют 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, создающие УБПДн;

- 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 (см. раздел 3.2 на стр. 20).

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;

- носитель вредоносной программы.

7.2 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.

7.2.1 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.

7.2.2 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 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 (список лиц должен быть уточнен в соответствии с группами пользователей описанных в Политике информационной безопасности):

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

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

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

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

7.2.3 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.

7.2.4 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 (информационные и управляющие интерфейсы СВТ);

- средств воздействия на источники и через цепи питания;

- средств воздействия через цепи заземления;

- средств активного воздействия на технические средства (средств облучения).

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

Необходимо определить всех потенциальных нарушителей, не имеющих доступа в ИСПДн. Потенциальных нарушителей и всех пользователей ИСПДн (см. раздел 4 на стр. 25) и определить их категорию.

7.3 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;

- несанкационированные 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).

7.4 Перечень возможных УБПДн

Для ИСПДн Учреждений 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.

Определение УБПДн производится на основании Отчета о результатах проведения внутренней проверки. Список УБПДн может быть скорректирован в зависимости от типа ИСПДн. Так, если ИСПДн не имеет подключения к сетям общего пользования и (или) международного обмена, то Угрозы несанкционированного доступа по каналам связи, можно убрать из общего списка угроз.

7.5 Определение вероятности 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 (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- **маловероятно -** отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

- **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

- **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

Определение вероятности реализации угрозы, должно быть проведено для всех выявленных угроз (см. раздел 8.3). Ниже приведено описание каждой угрозы и даны обобщенные вероятности реализации угроз для каждого типа ИСПДн.

7.5.1 Угрозы утечки информации по техническим каналам

7.5.1.1 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 наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн Учреждений функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют. Поэтому для всех типов ИСПДн вероятность реализации угрозы – **являются маловероятными.**

7.5.1.2 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.

Если в Учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи, то для всех типов ИСПДн вероятность реализации угрозы – **являются маловероятными.**

Если в Учреждении отсутствуют вышеперечисленные меры защиты, то их необходимо внедрить.

7.5.1.3 Угрозы утечки информации по каналам ПЭМИН

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

Угрозы данного класса **маловероятны** для всех типов ИСПДн, т.к. размер контролируемой зоны большой, и элементы ИСПДн, зачастую, находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов не входящих в ИСПДн.

7.5.2 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).

7.5.2.1 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 помещения, где расположены элементы ИСПДн.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД посторонних лиц в контролируемую зону.

Кража носителей информации

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

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной**.

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходи-

мо принять меры по пресечению НСД посторонних лиц к носителям информации.

Кража ключей и атрибутов доступа

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

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, организовано хранение ключей в сейфе и введена политика «чистого стола», то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной**.

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД посторонних лиц к ключам и атрибутам доступа.

Кражи, модификации, уничтожения информации

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

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону.

Вывод из строя узлов ПЭВМ, каналов связи

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

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону.

Несанкционированное отключение средств защиты

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

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, пользователи ИСПДн проинструктированы о работе с ПДн, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону и информированию пользователей о порядке работы в ИСПДн.

7.5.2.2 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.

Если в Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, то для всех типов ИСПДн вероятность реализации угрозы – **является низкой.**

При отсутствии установленной антивирусной защиты, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по предотвращению угроз вирусного заражения.

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 4.

Таблица 4

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.

Для снижения вероятности реализации угрозы необходимо сертифицировать ПО собственной разработки или стандартное ПО, доработанное под нужды учреждения.

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.

Если в учреждении введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При отсутствии разграничения прав на установку ПО, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по организации разграничения прав пользователей.

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

Если в Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, то для всех типов ИСПДн вероятность реализации угрозы – **является низкой.**

При отсутствии парольной политики или контроля за ее исполнением, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по организации парольной политики.

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.

Если в Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной**.

При отсутствии резервного копирования и неосведомленности пользователей о работе с ИСПДн, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

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.

Если 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, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При отсутствии контроля доступа в контролируемую зону и к настройкам режимов средств защиты, а так же неосведомленности пользователей о работе с ИСПДн, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

Выход из строя аппаратно-программных средств

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

Если в Учреждении осуществляет резервирование ключевых элементов ИСПДн, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При отсутствии резервирования ключевых элементов ИСПДн, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

Сбой системы электроснабжения

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

Если в Учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляет резервное копирование информации, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При отсутствии источников резервного питания и неосуществлении резервного копирования, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

Если в Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При отсутствии пожарной сигнализации и неосведомленности пользователей о действиях в случае возникновения внештатных ситуаций, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

7.5.2.4 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.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД посторонних лиц в контролируемую зону.

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.

Если в Учреждении пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении, то для всех типов ИСПДн вероятность реализации угрозы – **является низкой.**

При неосведомленности пользователей и не заключении Договора о неразглашении, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры снижению вероятности реализации угрозы.

7.5.2.5 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 с 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 5.

Таблица 5

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

Перехват в пределах контролируемой зоны внешними нарушителями

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону.

Перехват в пределах контролируемой зоны внутренними нарушителями.

Если в Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, то для всех типов ИСПДн вероятность реализации угрозы – **является маловероятной.**

При наличии свободного доступа в контролируемую зону посторонних лиц, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры по пресечению НСД в контролируемую зону.

Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

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	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

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 7.

Таблица 7

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

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 8.

Таблица 8

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

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 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

Внедрение ложного объекта сети

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

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

Угрозы типа «Отказ в обслуживании»

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

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

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

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	низкая	2
Распределенная ИС I типа	низкая	2
Распределенная ИС II типа	низкая	2

Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;

- удаленный запуск приложения путем переполнения буфера приложений-серверов;

- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

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 12.

Таблица 12

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

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 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

8 Реализуемость угроз

По итогам оценки уровня защищенности (Y_1) (раздел 7) и вероятности реализации угрозы (Y_2) (раздел 9), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (таблица 4). Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$

Определение реализуемости угроз производится на основании Отчета о результатах проведения внутренней проверки.

Обобщенный список оценки реализуемости УБПДн для разных типов ИСПДн представлен в таблицах 14-23.

Таблица 14 – Автономная ИС I типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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 переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	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 обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

Таблица 15 – Автономная ИС II типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая

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 переделами 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	0,35	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,25	низкая

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

Таблица 16 – Автономная ИС III типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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 переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	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 обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

Таблица 17 – Автономная ИС IV типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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	0,25	низкая

средств защиты		
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 переделами 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	0,35	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя

Таблица 18 – Автономная ИС V типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая

1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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	0,25	низкая

к ее обработке		
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 переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	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 обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

Таблица 19 – Автономная ИС VI типа

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 ин-		

формации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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 переделами 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	0,35	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя

Таблица 20 – ЛИС I типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая

2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,25	низкая
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 переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контроли-	0,25	низкая

руемой 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.	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 обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

Таблица 21 – ЛИС II типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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 переделами 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	0,35	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,35	средняя
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя

Таблица 22 – Распределенная ИС I типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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	0,35	средняя

персональных данных		
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 переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	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 обслужива-	0,35	средняя

нии»		
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

Таблица 23 – Распределенная ИС II типа

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	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 переделами 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.	0,35	средняя
2.5.3.Угрозы выявления паролей по сети	0,5	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,35	средняя
2.5.5.Угрозы подмены доверенного объекта в сети	0,35	средняя
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,35	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	0,35	средняя
2.5.8.Угрозы удаленного запуска приложений	0,5	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,5	средняя

9 Оценка опасности угроз

Оценка опасности 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.

Определение опасности угроз производится на основании Отчета о результатах проведения внутренней проверки.

Обобщенный список оценки опасности УБПДн для разных типов ИСПДн представлен в таблицах 24-33.

Таблица 24 – Автономная ИС I типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая
2.5.8.Угрозы удаленного запуска приложений	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая

Таблица 25 – Автономная ИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	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

Таблица 26 – Автономная ИС III типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними	низкая

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

Таблица 27 – Автономная ИС IV типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая

2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	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

Таблица 28 – Автономная ИС V типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации	

за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая
2.5.8.Угрозы удаленного запуска приложений	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая

Таблица 29 – Автономная ИС VI типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	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

Таблица 30 – ЛИС I типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая

2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая
2.5.8.Угрозы удаленного запуска приложений	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая

Таблица 31 – ЛИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	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

Таблица 32 – Распределенная ИС I типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3.Угрозы выявления паролей по сети	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая
2.5.8.Угрозы удаленного запуска приложений	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая

Таблица 33 – Распределенная ИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	высока
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	средняя
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	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) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	средняя
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.	средняя
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	средняя
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	средняя
2.5.8.Угрозы удаленного запуска приложений	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	высокая

10 Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной (таблица 34), для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 34

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

После чего делается вывод о наличии актуальных угроз и мер защиты, направленных на снижения риска возникновения и последствий актуальных угроз.

Определение актуальности угроз производится на основании Отчета о результатах проведения внутренней проверки.

После определения перечня актуальных угроз выбираются мероприятия организационного, физического технического и контролирующего характера по снижению опасности актуальных угроз. Перечень возможных мероприятий представлен в Плане мероприятий по обеспечению защиты ПДн.

Обобщенный список актуальных угроз, а так же предлагаемых мер защиты, для разных типов ИСПДн представлен в таблицах 35-42.

Таблица 35 – Автономная ИС I типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная

2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС I типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Таблица 36 – Автономная ИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
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

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа;
- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн и в сетях общего пользования и (или) международного обмена, а так же с ключами и атрибутами доступа;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Таблица 37 – Автономная ИС III типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС III типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа,.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Таблица 38 – Автономная ИС IV типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
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

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС IV типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Таблица 39 – Автономная ИС V типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС V типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Таблица 40 – Автономная ИС VI типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
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

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС VI типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Таблица 41 – ЛИС I типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная

2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

Таким образом, актуальными угрозами безопасности ПДн в ЛИС I типа, являются:

- грозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Таблица 42 – ЛИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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 переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
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

Таким образом, актуальными угрозами безопасности ПДн в ЛИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа;
- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Таблица 43 – Распределенная ИС I типа

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

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

Таким образом, актуальными угрозами безопасности ПДн в Распределенная ИС I типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- остановка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Таблица 44 – Распределенная ИС II типа

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. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. 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	актуальная
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 переделами с контролируемой зоны	актуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	актуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	актуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	актуальная
2.5.8.Угрозы удаленного запуска приложений	актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	актуальная

Таким образом, актуальными угрозами безопасности ПДн в Распределенная ИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы наличия недекларированных возможностей системного ПО и ПО для обработки персональных данных;

- угрозы утраты ключей и атрибутов доступа;

- угрозы перехвата за переделами с контролируемой зоны

- угрозы сканирования;

- угрозы выявления паролей по 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.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- 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;

- сертификация программных средств на НДВ;

- отключение элементов ИСПДн от сетей общего пользования и (или) международного обмена (сеть Интернет), если для функционирования ИСПДн не требуется такого подключения;

- осуществление резервирования ключевых элементов ИСПДн;

- организация физической защиты каналов передачи данных;

- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;

- 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.

Приложение 1
Обобщенная модель угроз для Автономной ИС I типа

Исходный класс защищенности – средний.

Таблица 45

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты

					Кодовый замок	
					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки

						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						

2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Пропускной режим Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Технологический процесс
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адре-	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности

сов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности

						Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС I типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- 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.

Приложение 2
Обобщенная модель угроз для Автономной ИС II типа

Исходный класс защищенности – средний.

Таблица 46

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления Генератор шума по цепи электропитания	Технологический процесс обработки Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация Решетки на окна Металлическая дверь Кодовый замок	Пропускной режим Охрана Акт установки средств защиты

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудни-	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование

ками						
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее об-	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

работке						
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;	Низкая	Средняя	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя

						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удален-	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс

ного запуска приложений.					Антивирусное ПО	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн и в сетях общего пользования и (или) международного обмена, а так же с ключами и атрибутами доступа;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Приложение 3
Обобщенная модель угроз для Автономной ИС III типа

Исходный класс защищенности – средний.

Таблица 47

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления Генератор шума по цепи электропитания	Технологический процесс обработки Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация Решетки на окна Металлическая дверь Кодовый замок	Пропускной режим Охрана Акт установки средств защиты

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) ин-	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование

формации сотрудниками						
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее об-	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

работке						
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;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя

						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удален-	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс

ного запуска приложений.					Антивирусное ПО	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС III типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа,.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Приложение 4
Обобщенная модель угроз для Автономной ИС IV типа

Исходный класс защищенности – средний.

Таблица 48

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты
					Кодовый замок	

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтоже-	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

ние 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;	Низкая	Средняя	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявле-	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс

ния паролей по сети.						Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Резервирование

2.5.8. Угрозы удаленного запуска приложений.	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС IV типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Приложение 5
Обобщенная модель угроз для Автономной ИС V типа

Исходный класс защищенности – средний.

Таблица 49

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты

					Кодовый замок	
					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки

						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
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 ат-	Низкая	Средняя	Средняя	Актуальная		Инструкция пользо-

рибутов доступа						вателя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за пределами с контролируемой зоны;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Пропускной режим Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Технологический процесс
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс

						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасно-

						сти
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС V типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Приложение 6
Обобщенная модель угроз для Автономной ИС VI типа

Исходный класс защищенности – средний.

Таблица 50

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты
					Кодовый замок	

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудни-	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование

ками						
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Низкая	Средняя	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности

						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Резервирование
2.5.8. Угрозы удаленного запуска прило-	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя

жений.						Инструкция администратора безопасности Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Автономной ИС VI типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Приложение 7
Обобщенная модель угроз для ЛИС I типа

Исходный класс защищенности – средний.

Таблица 51

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты

					Кодовый замок	
					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности

средств защиты						Технологический процесс обработки Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного

2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обра-	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска

ботке						Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Пропускной режим Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование Физическая зашита канала связи	Технологический процесс
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс Инструкция пользователя Инструкция администратора безопасности

станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс

как в ИСПДн, так и во внешних сетях.						Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Резервирование
2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в ЛИС I типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Приложение 8
Обобщенная модель угроз для ЛИС II типа

Исходный класс защищенности – средний.

Таблица 52

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты
					Кодовый замок	

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая	Средняя	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудни-	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование

ками						
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Низкая	Средняя	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности

						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удаленного запуска прило-	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя

жений.						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в ЛИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;

- назначить 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;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн.

Приложение 9
Обобщенная модель угроз для Распределенной ИС I типа

Исходный класс защищенности – средний.

Таблица 53

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты

					Кодовый замок	
					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки

						Акт установки 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)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая	Средняя	Низкая	Неактуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя

						Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя
						Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты
						Разрешительная система допуска
						Технологический процесс обработки
2.4.2. Разглашение информации, моди-	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении

фикация, уничтожение сотрудниками допущенными к ее обработке						Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявле-	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический про-

ния паролей по сети.						цесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности

						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Распределенная ИС I типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа.

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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.

Приложение 10
Обобщенная модель угроз для Распределенной ИС II типа

Исходный класс защищенности – средний.

Таблица 54

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя
						Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим
						Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления	Технологический процесс обработки
					Генератор шума по цепи электропитания	Контур заземления
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	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	Акт установки средств защиты
					Кодовый замок	

					Шифрование данных	
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Решетки на окна	
					Металлическая дверь	
					Кодовый замок	
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
					Решетки на окна	Охрана
					Металлическая дверь	
					Кодовый замок	
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки 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)	Низкая	Средняя	Высокая	Актуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая	Средняя	Средняя	Актуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Резервное копирование
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками до-	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя

пущенными 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;	Низкая	Средняя	Средняя	Актуальная	Шифрование	Технологический процесс
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Пропускной режим
					Физическая зашита канала связи	Технологический процесс
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование	Технологический процесс
					Физическая зашита канала связи	
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	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.3. Угрозы выявления паролей по сети.	Средняя	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя

						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.4. Угрозы навязывание ложного маршрута сети.	Низкая	Средняя	Низкая	Неактуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.5. Угрозы подмены доверенного объекта в сети.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
						Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
2.5.7. Угрозы типа «Отказ в обслуживании».	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс
					Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Резервирование
2.5.8. Угрозы удален-	Средняя	Средняя	Средняя	Актуальная	Межсетевой экран	Технологический процесс

ного запуска приложений.					Антивирусное ПО	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
2.5.9. Угрозы внедрения по сети вредоносных программ.	Средняя	Средняя	Высокая	Актуальная	Антивирусное ПО	Технологический процесс Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты

Таким образом, актуальными угрозами безопасности ПДн в Распределенная ИС II типа, являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы наличия недекларированных возможностей системного ПО и ПО для обработки персональных данных;

- угрозы перехвата за переделами с контролируемой зоны

- угрозы сканирования;

- угрозы утраты ключей и атрибутов доступа;

- угрозы выявления паролей по 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;

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить 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;

- сертификация программных средств на НДВ;

- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн;

- осуществление резервирования ключевых элементов ИСПДн;

- организация физической защиты каналов передачи данных;

- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;

- 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.