Утверждено приказом

ООО «ЛОУДЕР ЭСПИИКС»

№ ____ от «09» января 2023 г.

МОДЕЛЬ УГРОЗ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО «ЛОУДЕР ЭСПИИКС»

2023 год
Москва

АННОТАЦИЯ

Настоящий документ предназначен для обоснования выдвигаемых требований по обеспечению безопасности персональных данных и служит основой для проведения мероприятий по проектированию и внедрению системы защиты персональных данных в информационной системе персональных данных.

В ходе данной работы для информационных систем персональных данных ООО «ЛОУДЕР ЭСПИИКС» (далее – "ИСПДн") были определены:

1) Характерные параметры угроз:

– источники угроз;

– перечень характерных сценариев реализации угроз безопасности ПДн;

– объекты воздействия угроз;

– характер деструктивного воздействия на персональные данные;

– предпосылки реализации угроз;

– вероятность реализации угроз.

2) Возможности нарушителей, позволяющие определить класс криптосредств, в случае их использования в ИСПДн для обеспечения безопасности ПДн.

3) Актуальность угроз безопасности ПДн для рассматриваемой ИСПДн в соответствии с документом «Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021).

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4

2. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ 5

3. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ 6

3.1. Характеристики системы 6
3.2. Показатели опасности угроз 7
3.3. Реализованные защитные меры 8

4. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 11

4.1. Источники угроз безопасности персональных данных 11
4.2. Актуальность угроз, связанных с наличием недокументированных возможностей программного обеспечения 11
4.3. Перечень актуальных угроз безопасности персональных данных 11

ПРИЛОЖЕНИЕ А. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 12

ПРИЛОЖЕНИЕ Б. ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 14

Б.1. Угрозы, связанные с действиями внешнего нарушителя 14
Б.2. Угрозы, связанные с действиями внутреннего нарушителя 27
Б.3. Угрозы утечки по техническим каналам 58
Б.4. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе 63

ПРИЛОЖЕНИЕ В. МЕТОДИКА МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ 73

В.1. Порядок оценки актуальности угроз безопасности ПДн при их обработке в ИСПДн 73
В.2. Определение показателя исходной защищенности ИСПДн 73
В.3. Определение источников угроз 75
В.4. Формирование перечня объектов воздействия в ИСПДн 76
В.5. Формирование общего перечня УБПДн, характерного для анализируемой ИСПДн 76
В.6. Расчет параметров для угрозы и определение их актуальности 78

1. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Таблица 1. Условные обозначения и сокращения

Сокращение	Значение
АРМ	Автоматизированное рабочее место
ВТСС	Вспомогательные технические средства и системы
Д	Доступность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
К	Конфиденциальность
КЗ	Контролируемая зона
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения
СЗИ	Средство защиты информации
СФК	Среда функционирования криптосредств
УБПДн	Угроза безопасности персональных данных
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Ц	Целостность

2. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ

В ходе подготовки настоящего документа были использованы положения следующих нормативных документов:

1) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 15.02.2008).

2) "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021).

3) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4) Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден Приказом ФСТЭК России от 18.02 2013 № 21).

5) Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утвержден Приказом ФСБ России от 10.07.2014 № 378).

3. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Характеристики системы

Основные характеристики ИСПДн приведены в Таблице 1.

Таблица 1.

Основные характеристики ИСПДн

Наименование характеристики	Значение
Категория обрабатываемых персональных данных	Иные категории ПДн субъектов ПДн, являющихся сотрудниками оператора, а также иные категории ПДн субъектов ПДн, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	Менее 100 000 субъектов ПДн
Требуемые характеристики безопасности персональных данных (конфиденциальность/целостность/доступность)	Конфиденциальность, целостность, доступность
Структура информационной системы	Распределенная ИСПДн
Наличие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена	Имеет подключение к ССОП и СМИО
Режим обработки персональных данных	Многопользовательский
Наличие разграничения доступа	С разграничением прав доступа
Местонахождение технических средств информационной системы	Технические средства находятся на территории Российской Федерации и за ее пределами

Результаты определения уровня исходной защищенности ИСПДн, в соответствии с Приложением В к настоящему документу, представлены в Таблице 2.

Таблица 2.

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики	Уровень защищенности
По территориальному размещению	Высокий
По наличию соединения с сетями общего пользования	Средний
По встроенным операциям с записями	Низкий
По разграничению доступа	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
По уровню обобщения (обезличивания) ПДн	Средний
По объему ПДн, предоставляемых сторонним пользователям ИСПДн без предварительной обработки	Высокий

Согласно критериям, установленным [2], уровень исходной защищенности ИСПДн может быть оценен как средний, в связи с тем, что более **70%** характеристик ИСПДн соответствует среднему и высокому уровню защищенности, а остальные – низкому.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент, равный **5 (пяти)**.

3.2. Показатели опасности угроз

Последствия для субъектов ПДн при нарушении характеристик безопасности ПДн, обрабатываемых в ИСПДн, определенные решением Ответственного за организацию обработки персональных данных (Протокол определения показателей опасности угроз в ИСПДн ООО «ЛОУДЕР ЭСПИИКС»), представлен в Таблице 3.

Таблица 3.

Показатели опасности угроз в ИСПДн

Наименование характеристики безопасности ПДн	Размер последствий для субъекта ПДн	Показатель опасности угрозы
Конфиденциальность	Негативные последствия	Средняя опасность
Целостность	Незначительные негативные последствия	Низкая опасность
Доступность	Незначительные негативные последствия	Низкая опасность

3.3. Реализованные защитные меры

В ИСПДн используются технические средства защиты и приняты организационные меры, указанные в Таблице 4.

Таблица 4.

Реализованные защитные меры в ИСПДн

№	Наименование защитной меры	Используемые технические средства защиты и (или) организационные меры
Подсистема идентификации и аутентификации субъектов и объектов доступа		
1.	Идентификация и аутентификация пользователей, являющихся работниками оператора	Встроенные средства ОС и прикладного ПО
2.	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	
3.	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	
4.	Защита обратной связи при вводе аутентификационной информации	
5.	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	
Подсистема управления доступом субъектов к объектам доступа		
1.	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Встроенные средства ОС и прикладного ПО
2.	Реализация необходимых методов (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	
3.	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС	Коммутационное (сетевое) оборудование
4.	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС	Встроенные средства ОС и прикладного ПО

№	Наименование защитной меры	Используемые технические средства защиты и (или) организационные меры
5.	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	
6.	Ограничение неуспешных попыток входа в ИС (доступа к ИС)	
7.	Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу	
8.	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	
9.	Реализация защищенного удаленного доступа субъектов к объектам доступа через внешние информационно-телекоммуникационные сети	Доступ по VPN при наличие служебной необходимости
10.	Управление взаимодействием с ИС сторонних организаций (внешние ИС)	Взаимодействие с ИС сторонних организаций не осуществляется
Подсистема регистрации событий безопасности		
1.	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Встроенные средства ОС и прикладного ПО
2.	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	
3.	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	
4.	Защита информации о событиях безопасности	
Подсистема антивирусной защиты		
1.	Реализация антивирусной защиты	McAfee
2.	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Обновление базы данных осуществляется автоматически по мере выпуска обновлений производителем антивирусного средства защиты
Подсистема защиты технических средств		
1.	Контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены	Контроль физического доступа в помещения Компании осуществляется с помощью системы контроля и управления доступом (СКУД). Серверное помещение закрывается на ключ. Ключи имеются у руководителя отдела информационных технологий и системного администратора и в сейфе бухгалтерии

№	Наименование защитной меры	Используемые технические средства защиты и (или) организационные меры
2.	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Устройства вывода (отображения) информации размещены таким образом (например, к стене), что исключает возможность несанкционированного просмотра информации
Подсистема защиты информационной системы, ее средств, систем связи и передачи данных		
1.	Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи	–

4. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В ходе моделирования было установлено, что к актуальным угрозам относятся:

– угрозы, связанные с действиями внутренних нарушителей, имеющих доступ в КЗ, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн;

– угрозы, связанные с действиями внешних нарушителей, не имеющих доступа к ИСПДн.

4.1. Источники угроз безопасности персональных данных

Основными источниками угроз безопасности персональных данных в ИСПДн являются:

– внешний нарушитель;

– персонал, имеющий доступ в КЗ, но не имеющий доступа к защищаемой информации;

– персонал, имеющий легитимный доступ к защищаемой информации;

– поставщики аутсорсинговых услуг.

Детальное описание возможных источников угроз представлено в Приложении А к настоящему документу.

4.2. Актуальность угроз, связанных с наличием недокументированных возможностей программного обеспечения

В ходе моделирования угроз установлено, что для ИСПДн **неактуальны** угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т. е. **актуальны угрозы 3-го типа**.

4.3. Перечень актуальных угроз безопасности персональных данных

Результаты моделирования и оценки актуальности угроз безопасности ПДн представлены в Приложении Б к настоящему документу.

ПРИЛОЖЕНИЕ А. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Источниками угроз являются нарушители режима информационной безопасности в ИСПДн, т. е. лица (или инициируемый ими процесс), неумышленно нарушающие свойства безопасности информации, либо проводящие атаку на объекты воздействия ИСПДн.

Виды нарушителей в ИСПДн подразделяются:

– на внутренних нарушителей, имеющих доступ в ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн;

– на внешних нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из-за пределов контролируемой зоны.

Виды внешних и внутренних нарушителей, категории нарушителей и их возможности представлены в Таблице А.1.

Таблица А.1. Источники угроз ИБ

№ п/п	Вид нарушителя	Категория нарушителя	Тип нарушителя[1]	Возможности нарушителя
1	Внешний нарушитель	внешние субъекты (физические лица)	Н1	− может осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений; − может осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена; − может осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок; − может осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация)

[1]Категория и тип нарушителя определены в соответствии с документом «Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

				оказываются за пределами контролируемой зоны; − может осуществлять несанкционированные доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн; − располагает только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
2	Персонал, имеющий доступ в КЗ, но не имеющий доступа к защищаемой информации	лица, имеющие санкционированный доступ в КЗ, но не имеющие доступа к ПДн	Н1	− может располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; − может располагать именами и вести выявление паролей зарегистрированных пользователей; − располагает только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
3	Персонал, имеющий легитимный доступ к защищаемой информации	зарегистрированный пользователь ИР, имеющий ограниченные права доступа к ПДн ИСПДн с рабочего места	Н1	− может иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; − может располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; − может располагать именами и вести выявление паролей зарегистрированных пользователей; − знает, по меньшей мере, одно легальное имя доступа; − обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; − располагает конфиденциальными данными, к которым имеет доступ; − располагает только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
4	Поставщики аутсорсинговых услуг	лица, обеспечивающие сопровождение ИСПДн	Н1	− может располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; − может располагать именами и вести выявление паролей зарегистрированных пользователей; − располагает только доступными в свободной продаже аппаратными компонентами криптосредства и СФК

ПРИЛОЖЕНИЕ Б. ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Б.1. Угрозы, связанные с действиями внешнего нарушителя

Таблица Б.1. Угроза У-1

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Получение несанкционированного доступа к информации внешним нарушителем за счет внедрения вредоносного программного обеспечения</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><th colspan="7">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="7">Предпосылки:</th></tr>
<tr><td colspan="7">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении</td></tr>
<tr><th colspan="7">Реализованные защитные меры:</th></tr>
<tr><td colspan="7">- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;</td></tr>
</table>

- периодическое резервное копирование ПДн на резервные машинные носители ПДн
Вывод о вероятности реализации угрозы:
Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой

Таблица Б.2. Угроза У-2

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Получение несанкционированного доступа к информации внешним нарушителем за счет подбора/перехвата пароля доступа</td></tr>
<tr><th colspan="2">Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td colspan="2">К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- ограничение неуспешных попыток входа в ИС (доступа к ИС);
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- реализация защищенного удаленного доступа субъектов к объектам доступа через внешние информационно-телекоммуникационные сети;
- обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи;
- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
</table>

Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой

Таблица Б.3. Угроза У-3

Сценарий реализации угрозы				

<table>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем за счет внедрения ложного доверенного объекта и перенаправления сетевого соединения (трафика)</td><td rowspan="3">Вероятность реализации угрозы</td><td rowspan="3">Опасность угрозы</td><td rowspan="3">Возможность реализации угрозы</td><td rowspan="3">Актуальность угрозы</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Ц</td><td>5</td></tr>
<tr><td colspan="3">Объекты воздействия</td></tr>
<tr><td colspan="3">Информация, передаваемая по каналу связи</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- передача информации, содержащей персональные данные, через сети международного информационного обмена (сети связи общего пользования)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- реализация защищенного удаленного доступа субъектов к объектам доступа через внешние информационно-телекоммуникационные сети;
- обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.4. Угроза У-4

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем за счет перенаправления сетевого трафика путем изменения параметров работы сетевых устройств</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, передаваемая по каналу связи</td><td>Маловероятно</td><td>Средняя</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- передача информации, содержащей персональные данные, через сети международного информационного обмена (сети связи общего пользования)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- реализация защищенного удаленного доступа субъектов к объектам доступа через внешние информационно-телекоммуникационные сети;
- обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.5. Угроза У-5

<table>
<tr><td colspan="2">Сценарий реализации угрозы</td><td rowspan="4">Вероятность реализации угрозы</td><td rowspan="4">Опасность угрозы</td><td rowspan="4">Возможность реализации угрозы</td><td rowspan="4">Актуальность угрозы</td></tr>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем вследствие несанкционированного проникновения в помещения, в которых расположены носители информации, средства обработки информации, средства коммуникации</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Ц, Д</td><td>5</td></tr>
<tr><td colspan="6">Объекты воздействия</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
</table>

Предпосылки:
- наличие у нарушителя возможности проникновения в здание/помещение, в котором расположены средства обработки информации
Реализованные защитные меры:
- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены; - блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу; - разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации; - идентификация и аутентификация пользователей, являющихся работниками оператора; - реализация необходимых методов (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; - ограничение неуспешных попыток входа в ИС (доступа к ИС)
Вывод о вероятности реализации угрозы:
Вероятность реализации в свете отсутствия предпосылок, а также реализованных защитных мер считается низкой

Таблица Б.6. Угроза У-6

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем за счет воздействия на программное обеспечение (эксплуатация уязвимостей программного обеспечения)</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.7. Угроза У-7

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем за счет перехвата (прослушивания) трафика, передаваемого по каналу связи за пределами КЗ</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, передаваемая по каналу связи</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- передача информации, содержащей персональные данные, через сети международного информационного обмена (сети связи общего пользования);
- наличие у нарушителя доступа к каналу связи, выходящему за пределы контролируемой зоны</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- реализация защищенного удаленного доступа субъектов к объектам доступа через внешние информационно-телекоммуникационные сети;
- обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.8. Угроза У-8

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за перегрузки ресурсов (DOS/DDOS-атака) внешним нарушителем</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.9. Угроза У-9

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за уничтожения внешним нарушителем носителя информации за пределами контролируемой зоны</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="2">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.10. Угроза У-10

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Получение несанкционированного доступа к информации внешним нарушителем за счет хищения носителя информации за пределами контролируемой зоны</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Б.2. Угрозы, связанные с действиями внутреннего нарушителя

Таблица Б.11. Угроза У-11

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение, уничтожение, блокирование или изменение информации вследствие случайного или преднамеренного запуска/установки ПО, содержащего вредоносный код персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.12. Угроза У-12

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Разглашение, уничтожение, блокирование или изменение информации вследствие случайного или преднамеренного запуска/установки ПО, содержащего вредоносный код персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала возможности установки и запуска несанкционированного программного обеспечения;
- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.13. Угроза У-13

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации за счет загрузки альтернативной ОС с нештатного носителя персоналом, имеющим доступ в КЗ, но не имеющим доступа к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие возможности загрузки средств обработки информации с нештатного носителя;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.14. Угроза У-14

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Хищение информации за счет загрузки альтернативной ОС с нештатного носителя персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие возможности загрузки средств обработки информации с нештатного носителя;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.15. Угроза У-15

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации за счет загрузки альтернативной ОС с нештатного носителя со стороны персонала поставщика аутсорсинговых услуг</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала поставщика аутсорсинговых услуг, доступа к информации, средствам обработки информации;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие возможности загрузки средств обработки информации с нештатного носителя;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.16. Угроза У-16

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="3">Хищение информации за счет загрузки альтернативной ОС с нештатного носителя персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>К</td><td colspan="2">5</td></tr>
<tr><td colspan="3">Объекты воздействия</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие возможности загрузки средств обработки информации с нештатного носителя;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.17. Угроза У-17

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации вследствие воздействия на программное обеспечение (эксплуатирование уязвимостей, DOS-атака) персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="2">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.18. Угроза У-18

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации вследствие воздействия на программное обеспечение (эксплуатирование уязвимостей, DOS-атака) персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.19. Угроза У-19

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации со стороны персонала, имеющего доступ в КЗ, но не имеющего доступ к защищаемой информации, вследствие некорректного разграничения доступа (сетевого, файлового, на уровне приложений)</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- ограничение неуспешных попыток входа в ИС (доступа к ИС);
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.20. Угроза У-20

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации со стороны персонала поставщика аутсорсинговых услуг вследствие некорректного разграничения доступа (сетевого, файлового, на уровне приложений)</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала поставщика аутсорсинговых услуг, доступа к информации, средствам обработки информации;
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- ограничение неуспешных попыток входа в ИС (доступа к ИС);
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.21. Угроза У-21

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации со стороны персонала, имеющего доступ в КЗ, но не имеющего доступ к защищаемой информации, вследствие подключения несанкционированного оборудования к линиям связи (локальной сети)</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К</td><td>5</td></tr>
<tr><th colspan="2">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.22. Угроза У-22

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Несанкционированный доступ к информации со стороны персонала поставщика аутсорсинговых услуг вследствие подключения несанкционированного оборудования к линиям связи (локальной сети)</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала поставщика аутсорсинговых услуг, доступа к информации, средствам обработки информации;
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.23. Угроза У-23

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Несанкционированный доступ к информации со стороны персонала, имеющего доступ в КЗ, но не имеющего доступ к защищаемой информации, вследствие оставленных без присмотра незаблокированных терминалов (АРМ, серверов)</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу;
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.24. Угроза У-24

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Несанкционированный доступ к информации со стороны персонала поставщика аутсорсинговых услуг вследствие оставленных без присмотра незаблокированных терминалов (АРМ, серверов)</td></tr>
<tr><td>Нарушаемые свойства</td><td colspan="2">Исходная степень защищенности</td></tr>
<tr><td>К, Ц, Д</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><td colspan="3">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала поставщика аутсорсинговых услуг, доступа к информации, средствам обработки информации;
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- идентификация и аутентификация пользователей, являющихся работниками оператора;
- блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу;
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.25. Угроза У-25

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Разглашение информации вследствие случайного или преднамеренного копирования информации на несанкционированные носители (в т. ч. вывод на печать) персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>К</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала возможности копирования информации на несанкционированные носители (в т. ч. отправка на печать);
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль использования интерфейсов ввода (вывода) информации на машинные носители ПДн;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- защита информации о событиях безопасности</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.26. Угроза У-26

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение информации вследствие случайного или преднамеренного копирования информации на несанкционированные носители (в т. ч. вывод на печать) персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала возможности копирования информации на несанкционированные носители (в т. ч. отправка на печать);
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.27. Угроза У-27

<table>
<tr><td colspan="2">Сценарий реализации угрозы</td><td rowspan="4">Вероятность реализации угрозы</td><td rowspan="4">Опасность угрозы</td><td rowspan="4">Возможность реализации угрозы</td><td rowspan="4">Актуальность угрозы</td></tr>
<tr><td colspan="2">Несанкционированный доступ к информации за счет подбора и использования пароля привилегированного доступа персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Ц, Д</td><td>5</td></tr>
<tr><td colspan="2">Объекты воздействия</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- ограничение неуспешных попыток входа в ИС (доступа к ИС);
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.28. Угроза У-28

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение и (или) блокирование доступа к информации вследствие случайной потери носителя информации персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.29. Угроза У-29

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение и (или) блокирование доступа к информации вследствие случайной потери носителя информации персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.30. Угроза У-30

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения носителя информации, средств обработки информации персоналом, имеющим доступ в КЗ, но не имеющим доступа к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.31. Угроза У-31

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения носителя информации, средств обработки информации персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>Д</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.32. Угроза У-32

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения носителя информации, средств обработки информации персоналом поставщика аутсорсинговых услуг</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="2">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала поставщика аутсорсинговых услуг, доступа к информации, средствам обработки информации;
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.33. Угроза У-33

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="3">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения носителя информации, средств обработки информации персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>Д</td><td colspan="2">5</td></tr>
<tr><th colspan="3">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- неосторожное/небрежное обращение с носителями информации и средствами обработки информации (в т. ч. по незнанию);
- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.34. Угроза У-34

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения (стирания) информации персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th colspan="2">Исходная степень защищенности</th></tr>
<tr><td>Д</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- некорректная обработка/обращение с информацией со стороны персонала</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.35. Угроза У-35

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Уничтожение/блокирование доступа к информации из-за случайного или преднамеренного уничтожения (стирания) информации персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>Д</td><td>5</td></tr>
<tr><th colspan="2">Объекты воздействия</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- некорректная обработка/обращение с информацией со стороны персонала</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.36. Угроза У-36

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Неумышленное или преднамеренное разглашение информации за счет передачи ее за пределы организации с использованием сети Интернет (электронная почта, веб-доступ, сервисы мгновенного обмена сообщениями, файлообменные сети и пр.) персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Низкая</td><td>Низкая</td><td>Средняя</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие у персонала возможности установки и запуска несанкционированного программного обеспечения;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности передачи информации за пределы организации с использованием сети Интернет (в т. ч. электронной почты)</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается низкой</td></tr>
</table>

Таблица Б.37. Угроза У-37

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Неумышленное или преднамеренное разглашение информации за счет передачи ее за пределы организации с использованием сети Интернет (электронная почта, веб-доступ, сервисы мгновенного обмена сообщениями, файлообменные сети и пр.) персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие у персонала возможности установки и запуска несанкционированного программного обеспечения;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности передачи информации за пределы организации с использованием сети Интернет (в т. ч. электронной почты)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.38. Угроза У-38

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Разглашение/блокирование доступа к информации вследствие умышленного хищения носителя информации, средств обработки информации персоналом, имеющим доступ к КЗ, но не имеющим доступа к защищаемой информации</td></tr>
<tr><td>Нарушаемые свойства</td><td colspan="2">Исходная степень защищенности</td></tr>
<tr><td>К, Д</td><td colspan="2">5</td><td colspan="4"></td></tr>
<tr><td colspan="3">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.39. Угроза У-39

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Разглашение/блокирование доступа к информации вследствие умышленного хищения носителя информации, средств обработки информации, персоналом, имеющим легитимный доступ к защищаемой информации</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Д</td><td>5</td><td></td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.40. Угроза У-40

<table>
<tr><td colspan="2">Сценарий реализации угрозы</td><td rowspan="4">Вероятность реализации угрозы</td><td rowspan="4">Опасность угрозы</td><td rowspan="4">Возможность реализации угрозы</td><td rowspan="4">Актуальность угрозы</td></tr>
<tr><td colspan="2">Разглашение/блокирование доступа к информации вследствие умышленного хищения носителя информации, средств обработки информации персоналом, осуществляющим администрирование оборудования</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К, Д</td><td>5</td></tr>
<tr><td colspan="2">Объекты воздействия</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, содержащаяся на электронном или бумажном носителе информации</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.41. Угроза У-41

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Несанкционированный доступ к информации со стороны персонала поставщика аутсорсинговых услуг при проведении ремонтных работ средств обработки информации</td></tr>
<tr><td>Нарушаемые свойства</td><td colspan="2">Исходная степень защищенности</td></tr>
<tr><td>К</td><td colspan="2">5</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td colspan="3">Объекты воздействия</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие у персонала доступа к информации, носителям, средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">Отсутствуют</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Б.3. Угрозы утечки по техническим каналам

Таблица Б.42. Угроза У-42

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение информации за счет чтения внешним нарушителем информации с устройств отображения в служебных помещениях, либо с расстояния прямой видимости</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К</td><td>5</td><td colspan="4" rowspan="2"></td></tr>
<tr><th colspan="2">Объекты воздействия</th></tr>
<tr><td colspan="2">Технические средства ИСПДн и ВТСС</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие устройств отображения защищаемой информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены;
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.43. Угроза У-43

<table>
<tr><td colspan="2">Сценарий реализации угрозы</td><td rowspan="4">Вероятность реализации угрозы</td><td rowspan="4">Опасность угрозы</td><td rowspan="4">Возможность реализации угрозы</td><td rowspan="4">Актуальность угрозы</td></tr>
<tr><td colspan="2">Разглашение информации за счет чтения внешним нарушителем информации с устройств отображения на значительном расстоянии при помощи спецсредств</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td></tr>
<tr><td colspan="2">Объекты воздействия</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Технические средства ИСПДн и ВТСС</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие устройств отображения защищаемой информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.44. Угроза У-44

<table>
<tr><td colspan="2">Сценарий реализации угрозы</td><td rowspan="4">Вероятность реализации угрозы</td><td rowspan="4">Опасность угрозы</td><td rowspan="4">Возможность реализации угрозы</td><td rowspan="4">Актуальность угрозы</td></tr>
<tr><td colspan="2">Разглашение информации за счет снятия внешним нарушителем ПЭМИ с основных и вспомогательных технических средств за счет облучения и ВЧ-навязывания</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td></tr>
<tr><td colspan="2">Объекты воздействия</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Технические средства ИСПДн и ВТСС</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- излучение ПЭМИ техническими средствами ИСПДн в процессе работы</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">Отсутствуют</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.45. Угроза У-45

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение информации за счет снятия внешним нарушителем ПЭМИН информационного сигнала в цепях электропитания/заземления</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Технические средства ИСПДн и ВТСС</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- излучение ПЭМИ техническими средствами ИСПДн в процессе работы;
- наличие у нарушителя доступа к цепям электропитания/заземления</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">Отсутствуют</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.46. Угроза У-46

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Разглашение информации за счет снятия внешним нарушителем информационного сигнала при его передаче по каналу связи (электромагнитный/индукционный канал)</td></tr>
<tr><td>Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td>К</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="2">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="2">Технические средства ИСПДн и ВТСС</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие у нарушителя доступа к каналу связи, выходящему за пределы контролируемой зоны;
- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">Отсутствуют</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Б.4. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

Таблица Б.47. Угроза У-47

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование внешним нарушителем недокументированных (недекларированных) возможностей в системном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><th>Объекты воздействия</th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.48. Угроза У-48

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Использование персоналом, имеющим доступ в КЗ, но не имеющим доступа к защищаемой информации, недокументированных (недекларированных) возможностей в системном программном обеспечении</td></tr>
<tr><td colspan="2">Нарушаемые свойства</td><td>Исходная степень защищенности</td></tr>
<tr><td colspan="2">К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><td colspan="3">Объекты воздействия</td><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="7">Предпосылки:</td></tr>
<tr><td colspan="7">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="7">Реализованные защитные меры:</td></tr>
<tr><td colspan="7">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><td colspan="7">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.49. Угроза У-49

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="4">Вероятность реализации угрозы</th><th rowspan="4">Опасность угрозы</th><th rowspan="4">Возможность реализации угрозы</th><th rowspan="4">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом, имеющим легитимный доступ к защищаемой информации, недокументированных (недекларированных) возможностей в системном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td></tr>
<tr><th colspan="3">Объекты воздействия</th></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.50. Угроза У-50

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом, осуществляющим администрирование оборудования, недокументированных (недекларированных) возможностей в системном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="2">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.51. Угроза У-51

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом поставщика аутсорсинговых услуг недокументированных (недекларированных) возможностей в системном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала поставщика аутсорсинговых услуг доступа к информации, средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.52. Угроза У-52

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование внешним нарушителем недокументированных (недекларированных) возможностей в прикладном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования);
- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.53. Угроза У-53

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом, имеющим доступ в КЗ, но не имеющим доступа к защищаемой информации, недокументированных (недекларированных) возможностей в прикладном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.54. Угроза У-54

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом, имеющим легитимный доступ к защищаемой информации, недокументированных (недекларированных) возможностей в прикладном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.55. Угроза У-55

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2">Использование персоналом, осуществляющим администрирование оборудования, недокументированных (недекларированных) возможностей в прикладном программном обеспечении</td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td>К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="6">Объекты воздействия</th></tr>
<tr><td colspan="2">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="2">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="6">Предпосылки:</th></tr>
<tr><td colspan="6">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала доступа к информации, носителям, средствам обработки информации;
- наличие у персонала возможности подключения нештатных носителей к средствам обработки информации</td></tr>
<tr><th colspan="6">Реализованные защитные меры:</th></tr>
<tr><td colspan="6">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="6">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

Таблица Б.56. Угроза У-56

<table>
<tr><th colspan="3">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="3">Использование персоналом поставщика аутсорсинговых услуг недокументированных (недекларированных) возможностей в прикладном программном обеспечении</td></tr>
<tr><th colspan="2">Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td colspan="2">К, Ц, Д</td><td>5</td><td colspan="4"></td></tr>
<tr><th colspan="3">Объекты воздействия</th><td colspan="4"></td></tr>
<tr><td colspan="3">Информация, обрабатываемая на АРМ ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на серверах ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><td colspan="3">Информация, обрабатываемая на мобильном устройстве ИСПДн</td><td>Маловероятно</td><td>Низкая</td><td>Низкая</td><td>Не актуальна</td></tr>
<tr><th colspan="7">Предпосылки:</th></tr>
<tr><td colspan="7">- наличие уязвимостей, ошибок в прикладном и общесистемном программном обеспечении;
- наличие у персонала поставщика аутсорсинговых услуг доступа к информации, средствам обработки информации</td></tr>
<tr><th colspan="7">Реализованные защитные меры:</th></tr>
<tr><td colspan="7">- контроль установки обновлений ПО, включая обновление ПО СЗИ;
- периодическое резервное копирование ПДн на резервные машинные носители ПДн;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС</td></tr>
<tr><th colspan="7">Вывод о вероятности реализации угрозы:</th></tr>
<tr><td colspan="7">Вероятность реализации в свете наличия предпосылок, а также реализованных защитных мер считается маловероятной</td></tr>
</table>

ПРИЛОЖЕНИЕ В. МЕТОДИКА МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В.1. Порядок оценки актуальности угроз безопасности ПДн при их обработке в ИСПДн

Работы по оценке актуальности УБПДн проводятся по следующему алгоритму:

– определение показателя исходной защищенности ИСПДн;

– определение элементов описания угроз, актуальных для анализируемой ИСПДн;

– формирование перечня угроз;

– расчет вероятности реализации конкретной угрозы безопасности ПДн для данной ИСПДн исходя из предпосылок для реализации угрозы и принятых организационных и технических мер;

– расчет коэффициента реализуемости конкретной угрозы безопасности ПДн для данной ИСПДн;

– оценка опасности каждой конкретной угрозы безопасности ПДн для данной ИСПДн;

– определение актуальных угроз из полученного общего перечня УБПДн, характерных для анализируемой ИСПДн.

В.2. Определение показателя исходной защищенности ИСПДн

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

Таблица В.1. Характеристики ИСПДн для определения уровня исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению			
Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	–	–	+
Городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	–	–	+
Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	–	+	–

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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 обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	+	–	–

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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:

– Y1 = 0 – 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).

– Y1 = 5 – ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия предыдущего пункта, и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

– Y1 = 10 – ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия двух предыдущих пунктов.

Значение данного параметра вносится в столбец «Исходная степень защищенности» Таблицы В.3.

В.3. Определение источников угроз

Источниками угроз являются нарушители режима информационной безопасности в ИСПДн, то есть лица (или инициируемый ими процесс), проводящие атаку на объекты воздействия ИСПДн. Подробное описание источников угроз безопасности ПДн представлено в Приложении А.

В.4. Формирование перечня объектов воздействия в ИСПДн

Далее формируются перечни объектов воздействия, используемых в ИСПДн, характерные из них перечислены в Таблице В.2.

Таблица В.2. Объекты воздействия

Объект воздействия
Информация, обрабатываемая на АРМ ИСПДн
Информация, обрабатываемая на серверах ИСПДн
Информация, обрабатываемая на мобильных устройствах ИСПДн
Информация, содержащаяся на электронном или бумажном носителе информации
Информация, передаваемая в канале связи
Технические средства ИСПДн и ВТСС
Пользователь, осуществляющий голосовой ввод ПДн в ИСПДн
Акустическая система ИСПДн, воспроизводящая ПДн

В.5. Формирование общего перечня УБПДн, характерного для анализируемой ИСПДн

При формировании общего перечня УБПДн, характерного для анализируемой ИСПДн, рассматриваются угрозы возникающие в результате непреднамеренных или умышленных действий людей, способные привести к нарушению безопасности информации (антропогенные), угрозы, возникающие в процессе функционирования технических средств, способные вызвать нарушение безопасности информации (техногенные), а также угрозы, возникающие в результате различного природного или физического явления (наводнения, землетрясения, пожары и т. п.), способные привести к нарушению безопасности информации (природные).

Для каждой группы УБПДн создается описание, включающее в себя сводную информацию по наличию элементов описания угроз, характерных для анализируемой ИСПДн и определенных на предыдущих шагах настоящей методики, таких как источник угрозы, объект воздействия и последствия реализации угрозы. Данное описание имеет представление, отраженное в Таблице В.3.

В ходе моделирования угроз также учитываются предпосылки реализации угроз и принятые защитные меры: организационные и технические. Эти показатели влияют на определение вероятности реализации угроз. Расчет вероятности подробно описан в пункте В.6.1.

Таблица В.3. Форма таблицы оценки актуальности угроз безопасности ПДн в ИСПДн

<table>
<tr><th colspan="2">Сценарий реализации угрозы</th><th rowspan="3">Вероятность реализации угрозы</th><th rowspan="3">Опасность угрозы</th><th rowspan="3">Возможность реализации угрозы</th><th rowspan="3">Актуальность угрозы</th></tr>
<tr><td colspan="2"></td></tr>
<tr><th>Нарушаемые свойства</th><th>Исходная степень защищенности</th></tr>
<tr><td></td><td></td><td colspan="5">Объекты воздействия</td></tr>
<tr><td colspan="2"><Объект воздействия></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"><Объект воздействия></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"><Объект воздействия></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Предпосылки:</td></tr>
<tr><td colspan="6">Описание предпосылок к реализации угрозы</td></tr>
<tr><td colspan="6">Реализованные защитные меры:</td></tr>
<tr><td colspan="6">Описание предпринятых в ИСПДн защитных мер, позволяющих нейтрализовать угрозу</td></tr>
<tr><td colspan="6">Вывод о вероятности реализации угрозы:</td></tr>
<tr><td colspan="6">Вероятность реализации в свете наличия/отсутствия предпосылок, а также реализованных защитных мер считается низкой/средней/высокой.</td></tr>
</table>

В.6. Расчет параметров для угрозы и определение их актуальности

В.6.1. Расчет вероятности реализации УБПДн

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вводятся четыре вербальные градации этого показателя:

– Y2 = 0 – маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

– Y2 = 2 – низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (в организации внедрены средства защиты от данной угрозы и приняты организационные меры по минимизации возможности ее реализации);

– Y2 = 5 – средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (в организации не внедрены средства защиты от данной угрозы или не приняты организационные меры по минимизации возможности ее реализации);

– Y2 = 10 – высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (в организации не внедрены средства защиты от данной угрозы и не приняты организационные меры по минимизации возможности ее реализации).

Значение данного параметра вносится в столбец «Вероятность реализации угрозы» Таблицы В.3 для каждого объекта воздействия.

В.6.2. Оценка размера последствий для субъекта ПДн от реализации каждой УБПДн (опасности угроз)

Опасность угроз напрямую определяется теми последствиями для субъекта ПДн, к которым приводит их реализация. Последствия для субъекта ПДн определяются в виде показателя опасности угрозы. Критерии для определения размера последствий для субъекта ПДн и соответствующих показателей опасности угрозы определяются на основе опроса экспертов (специалистов в области защиты информации) и заносятся в документ «Протокол определения показателей опасности угроз в ИСПДн». Показатель опасности угрозы 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.

Значение данного параметра вносится в столбец «Опасность угрозы» Таблицы В.3 для каждого объекта воздействия.

В.6.3. Определение актуальных угроз из полученного общего перечня УБПДн, характерных для анализируемой ИСПДн

$Y = \frac{(Y1+Y2)}{20}$На данном этапе проводится экспертная оценка сформированных наборов угроз безопасности ПДн с точки зрения частоты (вероятности) их реализации с определением для каждой угрозы соответствующего числового коэффициента (Y2) и производится вычисление коэффициентов реализуемости выявленных угроз (Y) в соответствии с формулой:

с последующей вербальной интерпретацией полученных коэффициентов для всех выявленных угроз в диапазоне «низкая – средняя – высокая – очень высокая».

По итогам вычислений коэффициента реализуемости угрозы Y для каждой угрозы формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признается низкой;

– если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается средней;

– если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признается высокой;

– если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Значение данного параметра вносится в столбец «Возможность реализации угрозы» Таблицы В.5 для каждого объекта воздействия.

Далее определяется актуальность каждой УБПДн для ИСПДн в соответствии с правилами, приведёнными в [2], в соответствии с Таблицей В.4.

Таблица В.4. Таблица параметров определения актуальности УБПДн

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

Значение данного параметра вносится в столбец «Актуальность угрозы» Таблицы В.5 для каждого объекта воздействия.

Итогом моделирования угроз, проведенных в Приложении Б к настоящему документу, является Таблица 5 Раздела 4 «Актуальные угрозы безопасности персональных данных». В нее вносятся все актуальные угрозы с такими параметрами, как объект воздействия и последствия реализации угрозы.