ПРАВИТЕЛЬСТВО ПЕНЗЕНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 20 апреля 2017 года № 192-пП

г.Пенза

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Пензенской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями), в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, Правительство Пензенской области **п о с т а н о в л я е т:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Пензенской области, согласно приложению к настоящему постановлению.

2. Исполнительным органам государственной власти Пензенской области и подведомственным им организациям:

2.1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных, в течение трех месяцев с момента официального опубликования настоящего постановления.

2.2. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Настоящее постановление опубликовать в газете «Пензенские губернские ведомости» и разместить (опубликовать) на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и на официальном сайте Правительства Пензенской области в информационно-телекоммуникационной сети «Интернет».

4. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Правительства Пензенской области, координирующего вопросы информатизации.

Губернатор
Пензенской области И.А. Белозерцев

Приложение
к постановлению Правительства
Пензенской области
от 20 апреля 2017 года № 192-пП

АКТУАЛЬНЫЕ УГРОЗЫ
безопасности персональных данных при обработке в информационных системах персональных данных

1. Общие положения

1.1. Настоящий документ определяет перечень актуальных угроз безопасности персональных данных (далее – УБ ПДн) при обработке персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн), эксплуатируемых органами исполнительной власти и (или) местного самоуправления муниципальных районов и городских округов Пензенской области, и (или) подведомственными им организациями (далее – соответственно Органы, Организации), при осуществлении ими соответствующих видов деятельности, с учетом содержания ПДн, характера и способов их обработки. Данный перечень уточняется по мере выявления новых УБ ПДн и их источников, развития способов и средств их реализации.

1.2. В настоящем документе не рассматриваются вопросы обеспечения безопасности ПДн, отнесенные в установленном порядке к сведениям, составляющим государственную тайну.

1.3. Настоящий документ предназначен для Органов и Организаций при решении ими следующих задач:

- определение УБ ПДн, актуальных при обработке ПДн в ИСПДн;
- анализ защищенности ИСПДн от актуальных УБ ПДн в ходе выполнения мероприятий по информационной безопасности (защите информации);
- модернизация системы защиты ПДн в Органах и Организациях;
- проведение мероприятий по минимизации и (или) нейтрализации УБ ПДн;
- предотвращение несанкционированного воздействия на технические средства ИСПДн;
- контроль за обеспечением уровня защищенности ПДн.

1.4. При определении актуальных УБ ПДн при обработке ПДн в используемых ИСПДн и совокупности предположений о возможностях нарушителя, которые могут использоваться при создании, подготовке и проведении атак, Органы и Организации применяют с учетом категории ИСПДн, условий и особенностей функционирования ИСПДн, характера и способов обработки ПДн в ИСПДн типовые возможности нарушителей безопасности информации и направления атак, приведенные в приложении № 2 к настоящему документу, группы актуальных УБ ПДн в ИСПДн, приведенные в разделе 6 настоящего документа, и расширенный перечень УБ ПДн в ИСПДн, приведенный в приложении № 1 к настоящему документу, и согласно действующим методикам определения актуальных угроз безопасности информации осуществляют определение актуальных УБ ПДн.

1.5. Определение требований к системе защиты информации ИСПДн в зависимости от выявленного класса (уровня) защищенности ИСПДн и УБ ПДн, определенных в качестве актуальных при обработке ПДн в ИСПДн, и осуществление выбора средств защиты информации для системы защиты ПДн проводится в соответствии с нормативными правовыми актами, принятыми ФСБ России и ФСТЭК России во исполнение части 4 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.6. В документе дано описание:

- категорий ИСПДн как объектов защиты;
- объектов, защищаемых при определении УБ ПДн в ИСПДн;
- возможных источников УБ ПДн, обрабатываемых в ИСПДн;
- возможных видов неправомерных действий и деструктивных воздействий на ПДн в ИСПДн;
- основных способов реализации УБ ПДн.

1.7. В настоящем документе используются термины и понятия, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года, а также:

«ЕМСПД» – единая мультисервисная сеть передачи данных. Подключение к данной сети ее участников осуществляется с применением аппаратно-программных комплексов шифрования «Континент», обеспечивающих идентификацию и аутентификацию пользователей, доверенную загрузку, контроль целостности программной среды, ведение журнала регистрации событий, ведение системного журнала безопасности. Данная сеть позволяет обеспечить защиту ИСПДн всех уровней и классов защищенности уже на стадии создания;

«СВТ» – средства вычислительной техники;

«НСД» – несанкционированный доступ;

«НДВ» – недекларированные возможности;

«СПО» – системное программное обеспечение;

«ППО» – прикладное программное обеспечение;

«СЗИ» – средства защиты информации;

«СКЗИ» – средства криптографической защиты информации.

2. Владельцы и операторы ИСПДн, сети передачи данных

2.1. Владельцами ИСПДн и их операторами являются федеральные органы или Органы, или Организации.

2.2. Владельцы ИСПДн и их операторы расположены в пределах территории Российской Федерации.

2.3. Контролируемой зоной ИСПДн, функционирующих в Органах (Организациях), являются здания и отдельные помещения, принадлежащие им или арендуемые ими. Все СВТ, участвующие в обработке ПДн, располагаются в пределах контролируемой зоны Органа (Организации). Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование оператора связи (провайдера), используемое для информационного обмена по сетям связи общего пользования (сетям международного информационного обмена) и расположенное за пределами территории Органа (Организации).

2.4. Локальные вычислительные сети передачи данных в Органах и Организациях организованы по топологии «звезда» и имеют подключения к следующим сетям:

1) Внешним сетям (сетям провайдера). Подключение к внешним сетям организовано посредством следующих типов каналов связи:

- оптоволоконных каналов связи операторов связи (провайдеров);
- проводных каналов связи операторов связи (провайдеров).

2) Сетям Органов, Организаций и организаций (предприятий, учреждений), расположенных на территории Российской Федерации. Подключение к данным сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Органы исполнительной власти Пензенской области и администрации муниципальных районов и городских округов Пензенской области имеют подключение к ЕМСПД посредством защищенных каналов связи.

3) Иным сетям, взаимодействие с которыми организовано Органами и Организациями с целью исполнения своих полномочий.

2.5. Подключение к сетям связи общего пользования осуществляется Органами и Организациями при условии соблюдения ими мер по защите передаваемой информации, в том числе мер по защите подключения для передачи данных.

3. Объекты защиты и технологии обработки ПДн в ИСПДн

3.1. При определении Органами и Организациями УБ ПДн в конкретной ИСПДн защите подлежат как минимум следующие объекты, входящие в ИСПДн:

- ПДн, обрабатываемые в ИСПДн;
- информационные ресурсы ИСПДн (файлы, базы данных и т.п.);
- СВТ, участвующие в обработке ПДн посредством ИСПДн;
- СКЗИ;
- среда функционирования СКЗИ;
- информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;
- носители защищаемой информации, используемые в ИСПДн в том числе в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

- используемые ИСПДн каналы (линии) связи, включая кабельные системы;

- сети передачи данных, не выходящие за пределы контролируемой зоны ИСПДн;

- помещения, в которых обрабатываются ПДн посредством ИСПДн и располагаются компоненты ИСПДн;

- помещения, в которых находятся ресурсы ИСПДн, имеющие отношение к криптографической защите ПДн.

3.2. В состав СВТ, участвующих в обработке ПДн посредством ИСПДн, входят:

1) Автоматизированные рабочие места пользователей с различными уровнями доступа (правами) (далее – АРМ).

АРМ представляет собой программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к ИСПДн и предназначенный для локальной обработки информации.

2) Терминальная станция.

Терминальная станция представляет собой программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к ИСПДн, но не предназначенный для локальной обработки информации.

3) Серверное оборудование.

Серверное оборудование представляет собой программно-аппаратный комплекс в совокупности с программным и информационным обеспечением для его управления (общесистемное программное обеспечение (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.), прикладное программное обеспечение (системы управления базами данных и т.п.)), предназначенный для обработки и консолидированного хранения данных ИСПДн.

Серверное оборудование может быть представлено АРМ, выполняющими функции сервера.

4) Сетевое и телекоммуникационное оборудование.

Сетевое и телекоммуникационное оборудование представляет собой оборудование, используемое для информационного обмена между серверным оборудованием, АРМ, терминальными станциями (коммутаторы, маршрутизаторы и т.п.).

5) Общесистемное программное обеспечение (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.).

3.3. Ввод ПДн в ИСПДн в Органах и Организациях осуществляется как с бумажных носителей, так и с электронных носителей информации. ПДн выводятся из ИСПДн как в электронном, так и в бумажном виде с целью их хранения и (или) передачи третьим лицам.

4. ИСПДн

1) С целью исполнения своих полномочий Органами и Организациями обрабатываются все категории ПДн. Состав ПДн, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции), совершаемые с ПДн в ИСПДн, определяются Органом (Организацией), являющимся оператором ИСПДн.

2) Обработка ПДн в ИСПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Перечень обрабатываемых ПДн в ИСПДн соответствует целям их обработки.

3) ИСПДн подразделяются на:

- ИСПДн, оператором которых является сам Орган (Организация);
- ИСПДн, эксплуатируемые Органом (Организацией), но не в качестве ее оператора.

4) ИСПДн и ее компоненты расположены в пределах Российской Федерации.

5) ИСПДн подразделяются в зависимости от технологии обработки ПДн, целей и состава ПДн на следующие категории:

- информационно-справочные;
- сегментные;
- внутриобластные;
- ведомственные;
- служебные.

6) Для всех категорий ПДн вышеуказанных категорий ИСПДн необходимо обеспечивать следующие характеристики безопасности: конфиденциальность, целостность, доступность, подлинность.

7) В рамках ИСПДн возможна модификация и передача ПДн.

4.1. Информационно-справочные ИСПДн

4.1.1. Информационно-справочные ИСПДн используются для официального доведения любой информации до определенного или неопределенного круга лиц, при этом факт доведения такой информации не порождает правовых последствий, однако может являться обязательным в силу действующего законодательства.

4.1.2. К основным информационно-справочным ИСПДн относятся:

- официальные порталы (сайты) Органов и Организаций;
- информационные порталы (сайты), которые ведутся конкретным Органом (Организацией) и посвящаются определенному проекту и (или) мероприятию, проводимому на территории Пензенской области (далее – информационные порталы (сайты));
- закрытые порталы для нескольких групп участников Органов и Организаций;
- региональный интернет-портал государственных и муниципальных услуг (функций) Пензенской области.

4.1.3. **Официальные порталы (сайты) Органов и Организаций**.

4.1.3.1. Данные ИСПДн содержат сведения о деятельности Органов и Организаций, в том числе сведения, подлежащие обязательному опубликованию в данных ИСПДн в соответствии с действующим законодательством.

4.1.3.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

4.1.3.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется посредством веб-интерфейса сотрудниками Органа (Организации), являющегося оператором ИСПДн, и гражданами всех стран мира. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

4.1.3.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, и граждане всех стран мира.

4.1.3.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации), и (или) на серверном оборудовании иного Органа (Организации) в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

4.1.3.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

4.1.3.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.1.3.8. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 3.

4.1.4. **Информационные порталы (сайты)**.

4.1.4.1. Данные ИСПДн содержат сведения о мероприятиях, проводимых Органами (Организациями) в соответствии с функциями и полномочиями Органов (Организаций).

4.1.4.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

4.1.4.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется посредством веб-интерфейса сотрудниками Органа (Организации), являющегося оператором ИСПДн, и гражданами всех стран мира. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

4.1.4.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, и граждане всех стран мира.

4.1.4.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации), и (или) на серверном оборудовании иного Органа (Организации) в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

4.1.4.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

4.1.4.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.1.4.8. Характерные уровни защищенности ИСПДн: УЗ 4.

4.1.5. **Закрытые порталы для нескольких групп участников Органов и (или) Организаций**.

4.1.5.1. Данные ИСПДн содержат сведения, предоставляемые ограниченному круг лиц из числа Органов и (или) Организаций в соответствии с функциями и полномочиями Органов (Организаций).

4.1.5.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

4.1.5.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов и (или) Организаций посредством веб-интерфейса в соответствии с предоставленными правами. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

4.1.5.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органов и (или) Организаций.

4.1.5.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации), и (или) на серверном оборудовании иного Органа (Организации) в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

4.1.5.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

4.1.5.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.1.5.8. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 3.

4.1.6. **Региональный интернет-портал государственных и муниципальных услуг (функций) Пензенской области.**

4.1.6.1. Данная ИСПДн содержит социально значимую информацию и сведения, необходимые для получения гражданами государственных и муниципальных услуг в электронном виде.

4.1.6.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

4.1.6.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Органов (Организаций) и гражданами всех стран мира в режиме веб-интерфейса.

ПДн обрабатываются в деперсонифицированном (обезличенном) виде. Запрашиваемые данные не позволяют однозначно идентифицировать субъекта ПДн без использования сторонних баз данных. После получения запрашиваемых данных ИСПДн для получения ответа на запрос субъекта ПДн передает его данные по закрытым каналам связи в ИСПДн иных Органов (Организаций), в чью компетенцию входит предоставление информации по запросу субъекта. Ответ на запрос (сведения о ходе исполнения запроса) субъекта отображается в данной ИСПДн.

4.1.6.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, и граждане всех стран мира.

4.1.6.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации), и (или) на серверном оборудовании иного Органа (Организации) в пределах его контролируемой зоны, и (или) на вычислительных ресурсах облачного провайдера.

4.1.6.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

4.1.6.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.1.6.8. Характерные уровни защищенности ИСПДн: УЗ 4.

4.2. Сегментные ИСПДн

4.2.1. Сегментные ИСПДн представляют собой сегменты федеральных ИС, создаются и эксплуатируются на уровне Пензенской области на основании предоставляемых с федерального уровня рекомендаций (правовых, организационных, технических) и используются для сбора, обработки, свода данных на уровне Пензенской области и передачи их на уровень федеральный, и наоборот, при этом цели и задачи создания (модернизации), эксплуатации данных ИС определяются на федеральном уровне. Данные ИСПДн предназначены для реализации полномочий федеральных органов власти и исполнения функций Органов (Организаций).

4.2.2. К основным сегментным ИСПДн относятся:

- региональный сегмент Министерства здравоохранения Российской Федерации «Направление граждан на оказание высокотехнологичной медицинской помощи»;
- региональный банк данных о детях, оставшихся без попечения родителей, Министерства образования Пензенской области.

4.2.3. Обработке в ИСПДн могут подлежать все категории ПДн.

4.2.4. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса, и в отдельных случаях гражданами всех стран мира в режиме веб-интерфейса (с ограниченными правами доступа).

4.2.5. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: граждане всех стран мира.

4.2.6. Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Органа (Организации).

4.2.7. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

Обмен (передача и получение) ПДн с федеральным уровнем (федеральным сегментом), между региональными сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- посредством ЕМСПД;
- с использованием иных средств защиты информации, передаваемой по открытым каналам связи.

4.2.8. СВТ, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.2.9. **По технологии обработки** ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту, располагающемуся в пределах контролируемой зоны Органа (Организации), и передающее данные на центральный сегмент или напрямую в центральный;
- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;
- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте, располагающемся в пределах контролируемой зоны Органа (Организации) и передающем данные на центральный сегмент, или на центральном сегменте.

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) электронного сертификата, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) электронного сертификата, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.2.10. Характерные уровни защищенности ИСПДн: УЗ 3 – УЗ 1.

4.3. Внутриобластные ИСПДн

4.3.1. Внутриобластные ИСПДн создаются и эксплуатируются по желанию (на основании решения) Правительства Пензенской области (муниципальных образований, городских округов) или Органа (Организации) в интересах нескольких Органов (Организаций), при этом цели и задачи создания (модернизации), эксплуатации данных ИСПДн, а также требования к ним определяются на уровне Пензенской области (муниципальных образований, городских округов) или Органа (Организации) соответственно.

4.3.2. По выполняемым функциям ИСПДн подразделяются на:

- интеграционные (система межведомственного электронного взаимодействия Пензенской области (СМЭВ);
- многопрофильные (например, единая система электронного документооборота и делопроизводства органов исполнительной власти Пензенской области и органов местного самоуправления Пензенской области (СЭДД); автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг Пензенской области (АИС МФЦ);
- ИСПДн для Органов, Организаций и иных организаций (предприятий, учреждений) Пензенской области.

4.3.3. **ИСПДн интеграционные**.

4.3.3.1. Данные ИСПДн характеризуются отсутствием пользователей (кроме администраторов ИСПДн и администраторов безопасности ИСПДн) и функционируют исключительно в целях интеграции и передачи данных между ИСПДн иных категорий.

4.3.3.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные;
- общедоступные.

4.3.3.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.3.3.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: граждане всех стран мира.

4.3.3.5. Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа (Организации).

4.3.3.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

Обмен (передача и получение) ПДн с федеральным уровнем и с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- посредством ЕМСПД;

- с использованием иных средств защиты информации, передаваемой по открытым каналам связи.

4.3.3.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.3.3.8. Характерные уровни защищенности ИСПДн: УЗ 3 – УЗ 1.

4.3.4. **ИСПДн многопрофильные.**

4.3.4.1. Данная ИСПДн предназначена для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам и т.п. в Органах.

4.3.4.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;

- иные;

- общедоступные.

4.3.4.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах в соответствии с предоставленными правами.

4.3.4.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: граждане всех стран мира.

4.3.4.5. Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа (Организации).

4.3.4.6. ИСПДн подключена к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- подключенные посредством ЕМСПД;

- подключенные с использованием иных каналов связи.

Обмен (передача и получение) ПДн с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- посредством ЕМСПД;

- с использованием сторонних СКЗИ.

4.3.4.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.3.4.8. Характерные уровни защищенности ИСПДн: УЗ 3 – УЗ 2.

4.3.5. **ИСПДн для Органов, Организаций и иных организаций (предприятий, учреждений) Пензенской области**.

4.3.5.1. Данные ИСПДн предназначены для автоматизации совместной деятельности Органов, Организаций и иных организаций (предприятий, учреждений) Пензенской области, в том числе деятельности, которая необходима к исполнению в соответствии с требованиями действующего законодательства.

4.3.5.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;

- общедоступные.

4.3.5.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Органов (Организаций) и организациями (предприятиями, учреждениями) Пензенской области в специализированных программах в режиме веб-интерфейса.

4.3.5.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органов (Организаций) и организаций (предприятий, учреждений) Пензенской области.

4.3.5.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.3.5.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- подключенные посредством ЕМСПД;

- подключенные с использованием иных каналов связи.

Обмен (передача и получение) ПДн с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- посредством ЕМСПД;

- с использованием сторонних СКЗИ.

4.3.5.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.3.5.8. Характерные уровни защищенности ИСПДн: УЗ 3 – УЗ 2.

4.3.6. По архитектуре внутриобластные ИСПДн подразделяются на:

- сегментированные;

- централизованные;

- смешанные.

4.3.6.1. Сегментированные ИСПДн делятся на сегменты (центральный и периферийный), функционирующие независимо.

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

Периферийные сегменты являются непосредственно точками, которые отвечают за наполнение и первоначальную обработку информации. В состав периферийных сегментов входят АРМ, а также АРМ, выполняющий функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемой зоны АРМ, выполняющему функции сервера, или серверному оборудованию, осуществляющему консолидацию сведений на уровне периферийного сегмента, который в свою очередь передает полученные данные в центральный сегмент.

По технологии обработки ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к АРМ, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемой зоны Органа (Организации) и передающему данные на центральный сегмент;

- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемой зоны Органа (Организации) и передающем данные на центральный сегмент.

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.3.6.2. Централизованные ИСПДн делятся на сегменты (центральный и периферийный).

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

В состав периферийных сегментов входят только АРМ, которые являются непосредственно точками, которые отвечают за наполнение и первоначальную обработку информации. Пользователи периферийных сегментов подключаются напрямую к центральному сегменту и осуществляют обработку данных непосредственно на нем.

По технологии обработки ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;

- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.3.6.3. Смешанные ИСПДн построены с одновременным применением сегментированных и централизованных архитектур. Данные ИСПДн могут объединять в себе технологии обработки, характерные как для сегментированных ИСПДн, так и для централизованных ИСПДн.

4.4. Ведомственные ИСПДн

4.4.1. Ведомственные ИСПДн создаются (эксплуатируются) по решению Органа (Организации) в своих интересах и интересах подведомственных ему организаций (предприятий, учреждений), цели и задачи создания (модернизации), эксплуатации которых определяются Органом (Организацией). Ведомственные ИСПДн предназначены для исполнения функций Органов (Организаций).

4.4.2. К основным ведомственным ИСПДн относятся АИС ЗАГС.

4.4.3. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные.

4.4.4. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.4.5. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники оператора ИСПДн и иных Органов (Организаций), а также сторонние граждане.

4.4.6. Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Органа (Организации).

4.4.7. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

Обмен (передача и получение) ПДн между сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- посредством ЕМСПД;
- с использованием сторонних СКЗИ.

Также обмен ПДн между сегментами ИСПДн (при наличии) и с иными ИСПДн может осуществляться посредством собственных корпоративных сетей Органа (Организации).

4.4.8. СВТ, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.4.9. Характерные уровни защищенности ИСПДн: УЗ 3 – УЗ 1.

4.4.10. По архитектуре ведомственные ИСПДн подразделяются на:

- сегментированные;
- централизованные;
- смешанные.

4.4.10.1. Сегментированные ИСПДн делятся на сегменты (центральный и периферийный), функционирующие независимо.

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

Периферийные сегменты являются непосредственно точками, которые отвечают за наполнение и первоначальную обработку информации. В состав периферийных сегментов входят АРМ, а также АРМ, выполняющий функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенному в пределах контролируемой зоны АРМ, выполняющему функции сервера, или серверному оборудованию, осуществляющему консолидацию сведений на уровне периферийного сегмента, который в свою очередь передает полученные данные в центральный сегмент.

По технологии обработки ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к АРМ, выполняющему функции сервера, или серверному сегменту, располагающемуся в пределах контролируемой зоны Органа (Организации) и передающему данные на центральный сегмент;
- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемой зоны Органа (Организации) и передающем данные на центральный сегмент.

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.4.10.2. Централизованные ИСПДн делятся на сегменты (центральный и периферийный).

Центральный сегмент является единой точкой консолидации информации, получаемой от периферийных сегментов.

В состав периферийных сегментов входят только АРМ, которые являются непосредственно точками, которые отвечают за наполнение и первоначальную обработку информации. Пользователи периферийных сегментов подключаются напрямую к центральному сегменту и осуществляют обработку данных непосредственно на нем.

По технологии обработки ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту;

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее выгрузку данных на локальный носитель и последующую передачу выгруженных данных посредством защищенного канала связи или нарочно;

- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на центральном сегменте.

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.4.10.3. Смешанные ИСПДн построены с одновременным применением сегментированных и централизованных архитектур. Данные ИСПДн могут объединять в себе технологии обработки, характерные как для сегментированных ИСПДн, так и для централизованных ИСПДн.

4.5. Служебные ИСПДн

4.5.1. Служебные ИСПДн создаются (эксплуатируются) по желанию (на основании решения) Органа (Организации) и его лиц в интересах Органа (Организации) и его лиц, цели и задачи создания (модернизации), эксплуатации которых определяются Органом (Организацией), и используются для автоматизации определённой области деятельности или типовой деятельности, неспецифичной относительно полномочий конкретного Органа (Организации). Служебные ИСПДн предназначены для управления бизнес-процессами в Органе (Организации).

4.5.2. К основным служебным ИСПДн относятся:

- ИСПДн бухгалтерского учета и управления финансами;
- ИСПДн кадрового учета и управления персоналом;
- ИСПДн пенсионного фонда и налоговых служб;
- ИСПДн документооборота и делопроизводства;
- ИСПДн поддерживающие.

4.5.3. **ИСПДн бухгалтерского учета и управления финансами**.

4.5.3.1. Данные ИСПДн предназначены для автоматизации деятельности Органа (Организации), связанной с ведением бухгалтерского учета и управлением финансами.

4.5.3.2. Обработке в ИСПДн подлежат иные категории ПДн.

4.5.3.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.5.3.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн.

4.5.3.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.5.3.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- с использованием сторонних СКЗИ.

4.5.3.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.3.8. **По технологии обработки** ИСПДн подразделяются на:

- построенные по технологии толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере / АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа (Организации);
- построенные по технологии тонкого клиента: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте (сервере / АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа (Организации).

Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.3.9. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 3.

4.5.4. **ИСПДн кадрового учета и управления персоналом**.

4.5.4.1. Данные ИСПДн предназначены для автоматизации деятельности Органа (Организации), связанной с ведением кадрового учета и управления персоналом.

4.5.4.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;

- иные.

4.5.4.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных и (или) стандартных офисных программах, и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.5.4.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане Российской Федерации, устанавливающие (имеющие) трудовые отношения (трудовые договоры, служебные контракты) с Органом (Организацией).

4.5.4.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.5.4.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- подключенные посредством ЕМСПД;

- подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- с использованием сторонних СКЗИ.

4.5.4.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.4.8. **Технология обработки** ПДн в ИСПДн построена по принципу толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере / АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа (Организации). Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.4.9. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 2.

4.5.5. **ИСПДн пенсионного фонда и налоговых служб**.

4.5.5.1. Данные ИСПДн предназначены для автоматизации деятельности Органа (Организации), связанной с осуществлением пенсионных отчислений и уплатой налогов.

4.5.5.2. Обработке в ИСПДн подлежат иные категории ПДн.

4.5.5.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.5.5.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн.

4.5.5.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.5.5.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- подключенные посредством ЕМСПД;
- подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- с использованием сторонних СКЗИ.

4.5.5.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.5.8. **Технология обработки** ПДн в ИСПДн построена по принципу толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту (серверу / АРМ, выполняющему функцию сервера), располагающемуся вне контролируемой зоны Органа (Организации). Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.9. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 3.

4.5.6. **ИСПДн документооборота и делопроизводства**.

4.5.6.1. Данные ИСПДн предназначены для автоматизации деятельности Органа (Организации), связанной с осуществлением документооборота и делопроизводства.

4.5.6.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные;
- общедоступные.

4.5.6.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных программах в соответствии с предоставленными правами.

4.5.6.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, и граждане всех стран мира.

4.5.6.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.5.6.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- посредством ЕМСПД;

- с использованием сторонних СКЗИ.

4.5.6.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.6.8. **Технология обработки** ПДн в ИСПДн построена по принципу толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере / АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа (Организации). Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.6.9. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 2.

4.5.7. **ИСПДн поддерживающие**.

4.5.7.1. Данные ИСПДн предназначены для автоматизации деятельности Органа (Организации), связанной с осуществлением им (его сотрудниками) своих функций, полномочий и задач.

4.5.7.2. Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;

- иные;

- общедоступные.

4.5.7.3. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется сотрудниками Органов (Организаций) в специализированных и (или) стандартных офисных программах, и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

4.5.7.4. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, и граждане всех стран мира.

4.5.7.5. Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации).

4.5.7.6. ИСПДн подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения ИСПДн делятся на:

- без подключения (передача ПДн осуществляется с использованием машинных носителей);

- подключенные посредством ЕМСПД;

- подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн не осуществляется.

4.5.7.7. СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.7.8. **По технологии обработки** ИСПДн подразделяются на:

- построенные по принципу толстого клиента: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту (серверу / АРМ, выполняющему функцию сервера), располагающемуся в пределах контролируемой зоны Органа (Организации);

- построенные на базе стандартного офисного программного обеспечения: ИСПДн представляет собой базу данных в формате стандартного офисного приложения, обрабатываемую и хранящуюся на АРМ;

- построенные по веб-технологии: пользователи работают в ИСПДн посредством веб-интерфейса, подключающегося к локальному веб-серверу, располагающемуся в пределах контролируемой зоны Органа (Организации).

Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.7.9. Характерные уровни защищенности ИСПДн: УЗ 4 – УЗ 2.

5. УБ ПДн, выявленные при функционировании ИСПДн

5.1. Источники УБ ПДн.

Источниками УБ ПДн в ИСПДн выступают:

- носитель вредоносной программы;
- аппаратная закладка;
- нарушитель.

5.1.1. **Носитель вредоносной программы**.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW и т.п.), флэш-память, отчуждаемый винчестер и т.п.;

- встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода;

- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, файлами, имеющими определенные расширения или иные атрибуты, сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;

- файлы (текстовые, графические, исполняемые и т.д.).

5.1.2. **Аппаратная закладка**.

Потенциально может рассматриваться возможность применения аппаратных средств, предназначенных для регистрации вводимой в ИСПДн с клавиатуры АРМ информации (ПДн), например:

- аппаратная закладка внутри клавиатуры;
- считывание данных с кабеля клавиатуры бесконтактным методом;
- включение устройства в разрыв кабеля;
- аппаратная закладка внутри системного блока и др.

Однако в виду отсутствия возможности неконтролируемого пребывания физических лиц в служебных помещениях, в которых размещены технические средства ИСПДн, или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

5.1.3. **Нарушитель**.

Под нарушителем безопасности информации понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке в ИСПДн.

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на три типа:

- Внешний нарушитель. Данный тип нарушителя не имеет права постоянного или имеет право разового (контролируемого) доступа в КЗ, а также не имеет доступа к техническим средствам и ресурсам ИСПДн, расположенным в пределах КЗ, или он ограничен и контролируется. Данный тип нарушителя может реализовывать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- Внутренний нарушитель, имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа на территорию КЗ, а также доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах КЗ. Данный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн;
- Внутренний нарушитель, не имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа на территорию КЗ, но не имеет доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах КЗ. Данный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных.

5.2. Основные УБ ПДн в ИСПДн.

Основными группами УБ ПДн в ИСПДн являются:

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;

- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием облачных услуг;
- Угрозы, связанные с использованием суперкомпьютерных технологий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6. Актуальные УБ ПДн в ИСПДн

В настоящем разделе документа приведены группы актуальных УБ ПДн в ИСПДн из групп, указанных в пункте 5.2 настоящего документа, исходя из содержания ПДн, характера и способов их обработки.

6.1. Информационно-справочные ИСПДн.

6.1.1. **Официальные порталы (сайты) Органов и Организаций**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;

- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием облачных услуг;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.1.2. **Информационные порталы (сайты)**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием облачных услуг;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.1.3. **Закрытые порталы для нескольких групп участников Органов и (или) Организаций**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием облачных услуг;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.1.4. **Региональный интернет-портал государственных и муниципальных услуг (функций) Пензенской области**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием облачных услуг;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.2. Служебные ИСПДн.

6.2.1. **ИСПДн бухгалтерского учета и управления финансами**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;

- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.2.2. **ИСПДн кадрового учета и управления персоналом**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.2.3. **ИСПДн пенсионного фонда и налоговых служб**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.2.4. **ИСПДн документооборота и делопроизводства**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;

- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.2.5. **ИСПДн поддерживающие**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.3. Ведомственные ИСПДн.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.4. Внутриобластные ИСПДн.

6.4.1. **ИСПДн интеграционные**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.4.2. **ИСПДн многопрофильные**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.4.3. **ИСПДн для Органов, Организаций и иных организаций (предприятий, учреждений) Пензенской области**.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

6.5. Сегментные ИСПДн.

- Угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- Угрозы нарушения доступности информации;
- Угрозы нарушения целостности информации;
- Угрозы НДВ в СПО и ППО;
- Угрозы, не являющиеся атаками;
- Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;
- Угрозы ошибочных/деструктивных действий лиц;
- Угрозы нарушения конфиденциальности;
- Угрозы программно-математических воздействий;
- Угрозы, связанные с использованием технологий виртуализации;
- Угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- Угрозы физического доступа к компонентам ИСПДн;
- Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- Угрозы, связанные с использованием сетевых технологий;
- Угрозы инженерной инфраструктуры;
- Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- Угрозы, связанные с контролем защищенности ИСПДн;
- Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

7. Меры, направленные на минимизацию УБ ПДн в ИСПДн

При обработке ПДн в ИСПДн Органы (Организации) применяют правовые, организационные и технические меры, установленные Концепцией информационной безопасности Пензенской области и действующим законодательством, а также руководствуются положениями следующих нормативных правовых актов:

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

- постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении состава и содержания 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»;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15 февраля 2008 года;

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 14 февраля 2008 года;

- «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» Минздравсоцразвития России, согласованные с ФСТЭК России 22 декабря 2009 года;

- «Модель угроз типовой медицинской информационной системы (МИС) типового лечебного профилактического учреждения (ЛПУ)», Минздравсоцразвития России, согласованная с ФСТЭК России 27 ноября 2009 года;

- «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли», согласованная с ФСТЭК России, ФСБ России и одобренная Решением секции № 1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2;

- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация информационных систем и требования по защите информации», утвержденный решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года;

- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденные решением Коллегии Гостехкомиссии России №7.2/02.03.01;

- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№149/7/2/6-432 от 31 марта 2015 года).

Реализация правовых, организационных и технических мер, направленных на минимизацию УБ ПДн в ИСПДн, осуществляется специалистами по информационной безопасности (технической защите информации) Органов (Организаций), ответственными за планирование, организацию и реализацию мероприятий по обеспечению информационной безопасности в Органе (Организации).

Приложение №1
«Актуальные угрозы безопасности
персональных данных при обработке
в информационных системах
персональных данных»

П Е Р Е Ч Е Н Ь
угроз безопасности персональных данных в информационных системах персональных данных

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
1	2	3	4
1.	**Угрозы утечки информации по техническим каналам**		
1.1	**Угрозы утечки акустической информации**		
1.1.1	Использование направленных (ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.1.2	Использование «контактных микрофонов» для съема виброакустических сигналов	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.1.3	Использование «лазерных микрофонов» для съема виброакустических сигналов	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.1.4	Использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет «микрофонного эффекта» в ТС обработки информации и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений)	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.1.5	Применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки информации и ВТСС ВЧ-сигналом	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения

1	2	3	4
1.1.6	Применение акустооптических модуляторов на базе волоконно-оптической, находящихся в поле акустического сигнала («оптических микрофонов»)	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.2	**Угрозы утечки видовой информации**		
1.2.1	Визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИС	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.2.2	Визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИС	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.2.3	Использование специальных электронных устройств съема видовой информации (видеозакладки)	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.3	**Угрозы утечки информации по каналам ПЭМИН**		
1.3.1	Применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (программно-аппаратный комплекс (далее – ПАК), сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.3.2	Применение токосъемников для регистрации наводок информативного сигнала, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.3.3	Применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИС, или при наличии паразитной генерации в узлах ТС	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения
1.3.4	Применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИС, в которых проводится обработка информативных сигналов – параметрических каналов утечки	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с высоким потенциалом	Файлы БД системы, файлы сканов документов в виде электромагнитного излучения

1	2	3	4
2	**Угрозы использования штатных средств ИС с целью совершения НСД к информации**		
2.1	Угроза некорректного использования функционала программного обеспечения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение
2.2	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
2.3	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр
2.4	Угроза несанкционированного использования привилегированных функций BIOS	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI
2.5	Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ		
3.	**Угрозы нарушения доступности информации**		
3.1	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик
3.2	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Грид-система, сетевой трафик

1	2	3	4
3.3	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Гипервизор
3.4	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные
3.5	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Внутренний нарушитель с низким потенциалом	Система хранения данных суперкомпьютера
3.6	Угроза перегрузки грид-системы вычислительными заданиями	Внутренний нарушитель с низким потенциалом	Ресурсные центры грид-системы
3.7	Угроза повреждения системного реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, реестр
3.8	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик
3.9	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение
3.10	Угроза утраты вычислительных ресурсов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик
3.11	Угроза вывода из строя/выхода из строя отдельных технических средств*		
3.12	Угроза вывода из строя незарезервированных технических/программных средств/каналов связи		
3.13	Угроза отсутствия актуальных резервных копий информации*		

1	2	3	4
3.14	Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи*		
3.15	Угроза переполнения канала связи вследствие множества параллельных попыток авторизации*		
3.16	Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью*		
3.17	Угроза вывода из строя информационной системы при подаче на интерфейсы информационного обмена «неожидаемой» информации*		
4.	**Угрозы нарушения целостности информации**		
4.1	Угроза нарушения целостности данных кеша	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение
4.2	Угроза некорректного задания структуры данных транзакции	Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое программное обеспечение
4.3	Угроза переполнения целочисленных переменных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
4.4	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик
4.5	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Внутренний нарушитель с низким потенциалом	Информационная система, узлы хранилища больших данных
4.6	Угроза сбоя обработки специальным образом изменённых файлов	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное программное обеспечение
4.7	Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе средств защиты информации*		

1	2	3	4
4.8	Угроза отсутствия целостных резервных копий информации, программного обеспечения, средств защиты информации в случае реализации угроз информационной безопасности*		
4.9	Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми*		
4.10	Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми		
4.11	Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации		
4.12	Угроза доступа в ИС информации от неаутентифицированных серверов/пользователей		
4.13	Угроза отсутствия контроля за данными, передаваемыми из информационной системы*		
4.14	Отсутствие резервного копирования информации, передаваемой из ИС		
4.15	Угроза передачи из ИС недопустимой информации		
4.16	Угроза отсутствия контроля за данными, вводимыми в систему пользователями*		
4.17	Угроза ввода/передачи недостоверных/ошибочных данных*		
4.18	Угроза подмены используемых информационной системой файлов*		
4.19	Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты*		
4.20	Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения		
4.21	Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности		
4.22	Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе средств защиты информации		
4.23	Угроза отсутствия контроля целостности информации, обрабатываемой ИС, и ее структуры		

1	2	3	4
5.	**Угрозы НДВ в СПО и ППО**		
5.1	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
5.2	Угроза возникновения ошибок функционирования системного ПО, реализация недекларированных возможностей системного ПО		
5.3	Угроза использования встроенных недекларированных возможностей для получения несанкционированного доступа к ИС		
6.	**Угрозы, не являющиеся атаками**		
6.1	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Внутренний нарушитель с низким потенциалом	Информационная система
6.2	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные
6.3	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель с низким потенциалом	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр
6.4	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные
6.5	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные
6.6	Угроза выхода из строя/отказа отдельных технических, программных средств, каналов связи		
7.	**Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации**		
7.1	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI

1	2	3	4
7.2	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя
7.3	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение
7.4	Угроза программного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение
7.5	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение
7.6	Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации*		
7.7	Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации*		
7.8	Угроза получения несанкционированного доступа в результате сбоев/ошибок подсистемы идентификации и аутентификации*		
7.9	Угроза получения несанкционированного доступа сторонними лицами, устройствами*		
7.10	Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС		
7.11	Угрозы авторизации с использованием устаревших, но не отключённых учетных записей*		
7.12	Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа		
7.13	Угроза применения только программных методов двухфакторной аутентификации		
7.14	Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа		

1	2	3	4
7.15	Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических средств защиты информации		
7.16	Угроза доступа к ИС неаутентифицированных устройств и пользователей		
7.17	Угроза повторного использования идентификаторов в течение как минимум 1 года		
7.18	Угроза использования идентификаторов, не используемых более 45 дней		
7.19	Угроза раскрытия используемых идентификаторов пользователя в публичном доступе		
7.20	Отсутствие управления идентификаторами внешних пользователей		
7.21	Угроза использования «слабых»/предсказуемых паролей		
7.22	Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации		
7.23	Угроза использования пользователями идентичных идентификаторов в разных информационных системах		
7.24	Угроза использования неподписанных программных средств		
7.25	Угроза запуска несанкционированных процессов и служб от имени системных пользователей		
7.26	Угроза отсутствия регламента работы с персональными идентификаторами		
7.27	Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей		
7.28	Угроза бесконтрольного доступа пользователей к процессу загрузки		
7.29	Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования		

1	2	3	4
8.	**Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом**		
8.1	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик
8.2	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы
8.3	Угроза доступа к локальным файлам сервера при помощи URL	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение
8.4	Угроза загрузки нештатной операционной системы	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI
8.5	Угроза изменения режимов работы аппаратных элементов компьютера	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
8.6	Угроза изменения системных и глобальных переменных	Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.7	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение
8.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты

1	2	3	4
8.9	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.10	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
8.11	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI
8.12	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение
8.13	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, носители информации, объекты файловой системы
8.14	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации
8.15	Угроза несанкционированного доступа к системе по беспроводным каналам	Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение
8.16	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации
8.17	Угроза несанкционированного редактирования реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, использующее реестр, реестр
8.18	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение

1	2	3	4
8.19	Угроза несанкционированного управления буфером	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.20	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение
8.21	Угроза несанкционированного управления указателями	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.22	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение
8.23	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, аппаратное обеспечение
8.24	Угроза перехвата привилегированного потока	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.25	Угроза перехвата привилегированного процесса	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
8.26	Угроза повышения привилегий	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение, информационная система

1	2	3	4
8.27	Угроза подбора пароля BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI
8.28	Угроза подделки записей журнала регистрации событий	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение
8.29	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных		Информационная система, система разграничения доступа хранилища больших данных
8.30	Угроза удаления аутентификационной информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя
8.31	Угроза «форсированного веб-браузинга»	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение
8.32	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение
8.33	Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя*		
8.34	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами/учетными записями, в том числе с повышенными правами доступа*		
8.35	Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа*		
8.36	Угроза бесконтрольной передачи данных как внутри ИС, так и между ИС*		
8.37	Угроза получения дополнительных данных, не предусмотренных технологией обработки*		

1	2	3	4
8.38	Угроза получения разными пользователями, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенным для данных лиц, в связи с их должностными обязанностями*		
8.39	Угроза предоставления прав доступа, не являющихся необходимыми для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий*		
8.40	Отсутствие ограничения на количество неудачных попыток входа в информационную систему*		
8.41	Угроза использования (подключения) к открытому (незаблокированному) сеансу пользователя*		
8.42	Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации*		
8.43	Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа*		
8.44	Угроза подбора идентификационных данных для удаленного доступа к ИС*		
8.45	Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа*		
8.46	Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств*		
8.47	Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств, без прохождения процедуры идентификации и авторизации*		
8.48	Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств*		
8.49	Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем*		

1	2	3	4
8.50	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами/учетными записями, в том числе с повышенными правами доступа*		
8.51	Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации*		
8.52	Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей*		
8.53	Угроза бесконтрольного доступа к информации неопределенного круга лиц*		
8.54	Угроза получения доступа к данным, не предназначенным для пользователя*		
8.55	Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей*		
8.56	Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами*		
8.57	Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств*		
8.58	Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты		
8.59	Отсутствие отказоустойчивых централизованных средств управления учетными записями		
8.60	Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД		

1	2	3	4
8.61	Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации		
8.62	Угроза передачи информации разной степени конфиденциальности без разграничения информационных потоков		
8.63	Угроза передачи информации без соблюдения атрибутов (меток) безопасности, связанных с передаваемой информацией		
8.64	Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки передаваемых данных		
8.65	Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными		
8.66	Угроза несанкционированного доступа к средствам управления информационными потоками		
8.67	Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо		
8.68	Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним		
8.69	Отсутствие информирования пользователя о применении средств защиты информации и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа		
8.70	Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями		
8.71	Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств		

1	2	3	4
8.72	Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия – 5 минут		
8.73	Угроза использования незавершенных сеансов пользователей		
8.74	Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа		
8.75	Отсутствие автоматизированного мониторинга и контроля удаленного доступа		
8.76	Угроза использования уязвимых/незащищенных технологий удаленного доступа		
8.77	Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты		
8.78	Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации		
8.79	Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации		
8.80	Отсутствие контроля за используемыми интерфейсами ввода/вывода		
9.	**Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы информационной безопасности ИС**		
9.1	Угроза передачи данных по скрытым каналам	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
9.2	Угроза включения в проект не испытанных достоверно компонентов	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры

1	2	3	4
9.3	Угроза внедрения системной избыточности	Внутренний нарушитель со средним потенциалом	Программное обеспечение, информационная система, ключевая система информационной инфраструктуры
9.4	Угроза ошибок при моделировании угроз и нарушителей информационной безопасности*		
9.5	Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности*		
10.	**Угрозы ошибочных/деструктивных действий лиц**		
10.1	Угроза подмены действия пользователя путём обмана	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение
10.2	Угроза «фишинга»	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик
10.3	Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СрЗИ и СКЗИ в соответствии с установленными для них административными полномочиями*		
10.4	Внесение изменений в конфигурацию программных и технических средств в соответствии с установленными полномочиями, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ЕСЭДД, СЗИ (в случае сговора с внешними нарушителями безопасности информации)*		
10.5	Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС*		
10.6	Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС*		
10.7	Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления*		

1	2	3	4
10.8	Хищение ключей шифрования, идентификаторов и известных паролей*		
10.9	Внесение программно-аппаратных закладок в программно-аппаратные средства ИС, обеспечивающих съем информации, с использованием непосредственного подключения к техническим средствам обработки информации*		
10.10	Создание методов и средств реализации атак, а также самостоятельное проведение атаки		
10.11	Ошибки при конфигурировании и обслуживании модулей/компонентов ИС		
10.12	Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений)		
10.13	Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети		
10.14	Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним		
10.15	Нарушение правил хранения ключевой информации		
10.16	Передача защищаемой информации по открытым каналам связи		
10.17	Несанкционированная модификация/уничтожение информации легитимным пользователем		
10.18	Копирование информации на незарегистрированный носитель информации, в том числе печать		
10.19	Несанкционированное отключение средств защиты		
10.20	Угрозы вербовки (социальной инженерии)		
11.	**Угрозы нарушения конфиденциальности**		
11.1	Угроза исследования механизмов работы программы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение

1	2	3	4
11.2	Угроза исследования приложения через отчёты об ошибках	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение
11.3	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
11.4	Угроза обнаружения хостов	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
11.5	Угроза определения типов объектов защиты	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
11.6	Угроза определения топологии вычислительной сети	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
11.7	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение
11.8	Угроза получения сведений о владельце беспроводного устройства	Внешний нарушитель с низким потенциалом	Сетевой узел, метаданные
11.9	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой узел
11.10	Сканирование сети для изучения логики работы ИС, выявления протоколов, портов*		
11.11	Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе идентификаторов и паролей), их подмены*		
11.12	Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора)*		
11.13	Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты		
11.14	Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС		

1	2	3	4
11.15	Угроза получения нарушителем идентификационных данных легальных пользователей ИС		
11.16	Разглашение сведений конфиденциального характера		
12	**Угрозы программно-математических воздействий**		
12.1	Угроза автоматического распространения вредоносного кода в грид-системе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы
12.2	Угроза внедрения кода или данных	Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
12.3	Угроза восстановления аутентификационной информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя
12.4	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр
12.5	Угроза избыточного выделения оперативной памяти	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение
12.6	Угроза искажения XML-схемы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик

1	2	3	4
12.7	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение
12.8	Угроза использования слабостей кодирования входных данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр
12.9	Угроза межсайтового скриптинга	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение
12.10	Угроза межсайтовой подделки запроса	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение
12.11	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
12.12	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение
12.13	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
12.14	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
12.15	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение
12.16	Угроза неправомерного шифрования информации	Внешний нарушитель с низким потенциалом	Объект файловой системы
12.17	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение

1	2	3	4
12.18	Угроза распространения «почтовых червей»	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение
12.19	Внедрение программных закладок/закладок*		
12.20	Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа*		
12.21	Применение специально созданных программных продуктов для НСД*		
12.22	Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения*		
12.23	Отсутствие централизованной системы управления средствами антивирусной защиты		
13	**Угрозы, связанные с использованием облачных услуг**		
13.1	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Внутренний нарушитель с низким потенциалом	Облачная система, виртуальная машина
13.2	Угроза злоупотребления доверием потребителей облачных услуг	Внешний нарушитель с низким потенциалом	Облачная система
13.3	Угроза конфликта юрисдикций различных стран	Внешний нарушитель с низким потенциалом	Облачная система
13.4	Угроза нарушения доступности облачного сервера	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, облачный сервер
13.5	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Внешний нарушитель с низким потенциалом	Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение
13.6	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы
13.7	Угроза незащищённого администрирования облачных услуг	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, рабочая станция, сетевое программное обеспечение

1	2	3	4
13.8	Угроза некачественного переноса инфраструктуры в облако	Внешний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, облачная система
13.9	Угроза неконтролируемого роста числа виртуальных машин	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура
13.10	Угроза некорректной реализации политики лицензирования в облаке	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
13.11	Угроза неопределённости в распределении ответственности между ролями в облаке	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение
13.12	Угроза неопределённости ответственности за обеспечение безопасности облака	Внешний нарушитель с низким потенциалом	Облачная система
13.13	Угроза непрерывной модернизации облачной инфраструктуры	Внутренний нарушитель со средним потенциалом	Облачная инфраструктура
13.14	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, облачная система
13.15	Угроза общедоступности облачной инфраструктуры	Внешний нарушитель со средним потенциалом	Объекты файловой системы, аппаратное обеспечение, облачный сервер
13.16	Угроза потери доверия к поставщику облачных услуг	Внутренний нарушитель со средним потенциалом	Объекты файловой системы, информационная система, иммигрированная в облако
13.17	Угроза потери и утечки данных, обрабатываемых в облаке	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, метаданные, объекты файловой системы
13.18	Угроза потери управления облачными ресурсами	Внешний нарушитель с высоким потенциалом	Сетевой трафик, объекты файловой системы

1	2	3	4
13.19	Угроза потери управления собственной инфраструктурой при переносе её в облако	Внутренний нарушитель со средним потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
13.20	Угроза привязки к поставщику облачных услуг	Внутренний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы
13.21	Угроза приостановки оказания облачных услуг вследствие технических сбоев		Системное программное обеспечение, аппаратное обеспечение, канал связи
13.22	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная инфраструктура, созданная с использованием технологий виртуализации
14.	**Угрозы, связанные с использованием суперкомпьютерных технологий**		
14.1	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера
14.2	Угроза несанкционированного доступа к сегментам вычислительного поля	Внутренний нарушитель со средним потенциалом	Вычислительный узел суперкомпьютера
14.3	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Вычислительные узлы суперкомпьютера, каналы передачи данных суперкомпьютера, системное программное обеспечение
14.4	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера

1	2	3	4
15.	**Угрозы, связанные с использованием технологий виртуализации**		
15.1	Угроза выхода процесса за пределы виртуальной машины	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины
15.2	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальная машина, гипервизор
15.3	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина
15.4	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сервер
15.5	Угроза несанкционированного доступа к виртуальным каналам передачи	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства
15.6	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные
15.7	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина
15.8	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина

1	2	3	4
15.9	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальные устройства хранения, обработки и передачи данных
15.10	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальные устройства хранения данных, виртуальные диски
15.11	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, объекты файловой системы
15.12	Угроза ошибки обновления гипервизора	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, гипервизор
15.13	Угроза перехвата управления гипервизором	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, гипервизор, консоль управления гипервизором
15.14	Угроза перехвата управления средой виртуализации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение
15.15	Нарушение доверенной загрузки виртуальных серверов ИС, перехват загрузки*		
15.16	Нарушение целостности конфигурации виртуальных серверов – подмена/искажение образов (данных и оперативной памяти) *		
15.17	Несанкционированный доступ к консоли управления виртуальной инфраструктурой*		
15.18	Несанкционированный доступ к виртуальному серверу ИС, в том числе несанкционированное сетевое подключение и проведение сетевых атак на виртуальный сервер ИС*		

1	2	3	4
15.19	Несанкционированный удаленный доступ к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера»*		
15.20	Угроза несанкционированного доступа к объектам виртуальной инфраструктуры без прохождения процедуры идентификации и аутентификации*		
15.21	Угроза несанкционированного доступа к виртуальной инфраструктуре/компонентам виртуальной инфраструктуры/виртуальным машинам/объектам внутри виртуальных машин*		
15.22	Угроза отсутствия средств регистрации событий в виртуальной инфраструктуре*		
16.	**Угрозы, связанные с нарушением правил эксплуатации машинных носителей**		
16.1	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Машинный носитель информации
16.2	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Метаданные, объекты файловой системы, реестр
16.3	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом	Носитель информации
16.4	Угроза форматирования носителей информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Носитель информации
16.5	Повреждение носителя информации		
16.6	Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)		
16.7	Угроза подключения к ИС неучтенных машинных носителей*		
16.8	Угроза подключения к ИС неперсонифицированных машинных носителей		

1	2	3	4
16.9	Угроза несанкционированного копирования информации на машинные носители*		
16.10	Угроза несанкционированной модификации/удаления информации на машинных носителях*		
16.11	Угроза хищения машинных носителей*		
16.12	Угроза подмены машинных носителей*		
16.13	Угроза встраивания программно-аппаратных закладок в машинные носители*		
16.14	Угроза несанкционированного доступа к информации, хранящейся на машинном носителе*		
16.15	Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки		
16.16	Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители*		
16.17	Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей*		
16.18	Угроза несанкционированного использования машинных носителей		
16.19	Угроза несанкционированного выноса машинных носителей за пределы КЗ		
17	**Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования**		
17.1	Угроза внедрения вредоносного кода в BIOS	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
17.2	Угроза изменения компонентов системы	Внутренний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение
17.3	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Внешний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI

1	2	3	4
17.4	Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов*		
17.5	Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения*		
17.6	Установка программного обеспечения, содержащего известные уязвимости*		
17.7	Установка нелицензионного программного обеспечения*		
17.8	Угроза ошибочного запуска/установки программного обеспечения*		
17.9	Угроза неправильной установки программного обеспечения*		
17.10	Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске операционной системе и(или) обновлений программного обеспечения		
17.11	Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения		
17.12	Угроза несанкционированного запуска программного обеспечения в нерабочее время		
18.	**Угрозы физического доступа к компонентам ИС**		
18.1	Угроза преодоления физической защиты	Внешний нарушитель со средним потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
18.2	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
18.3	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
18.4	Угроза несанкционированного доступа к системам криптографической защиты информации *		
18.5	Угроза нарушения функционирования НЖМД и других систем хранения данных*		

1	2	3	4
18.6	Угроза доступа к системам обеспечения, их повреждение*		
18.7	Угроза нарушения функционирования кабельных линий связи, ТС*		
18.8	Угроза несанкционированного доступа в КЗ*		
18.9	Отсутствие средств автоматизированного контроля доступа		
19.	**Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИС, микропрограммном обеспечении**		
19.1	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение
19.2	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI
19.3	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI
19.4	Угроза использования поддельных цифровых подписей BIOS	Внешний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
19.5	Угроза использования слабых криптографических алгоритмов BIOS	Внешний нарушитель с высоким потенциалом	Микропрограммное обеспечение BIOS/UEFI
19.6	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства
19.7	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Внешний нарушитель со средним потенциалом	Узлы грид-системы
19.8	Угроза отключения контрольных датчиков	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение
19.9	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение
19.10	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы, узлы грид-системы, грид-система, сетевое программное обеспечение

1	2	3	4
19.11	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи
19.12	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI
19.13	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение
19.14	Угроза наличия механизмов разработчика	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство
19.15	Угроза «спама» веб-сервера	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение
20	**Угрозы, связанные с использованием сетевых технологий**		
20.1	Угроза деавторизации санкционированного клиента беспроводной сети	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел
20.2	Угроза заражения DNS-кеша	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик
20.3	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик
20.4	Угроза неправомерных действий в каналах связи	Внешний нарушитель с низким потенциалом	Сетевой трафик
20.5	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение
20.6	Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение

1	2	3	4
20.7	Угроза подмены беспроводного клиента или точки доступа	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка беспроводного доступа
20.8	Угроза подмены доверенного пользователя	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение
20.9	Угроза подмены субъекта сетевого доступа	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик
20.10	Угроза «фарминга»	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик
20.11	Угроза агрегирования данных, передаваемых в грид-системе	Внешний нарушитель со средним потенциалом	Сетевой трафик
20.12	Угроза удаленного запуска приложений		
20.13	Угроза навязывания ложных маршрутов*		
20.14	Угроза внедрения ложных объектов сети*		
20.15	Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа*		
20.16	Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений*		
20.17	Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений*		
20.18	Угроза отсутствия системы анализа сетевого трафика между сегментами информационной системы на наличие атак/вторжений*		
20.19	Угроза использования неактуальных версий сигнатур обнаружения атак*		
20.20	Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений		
20.21	Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа*		

1	2	3	4
20.22	Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств*		
20.23	Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа*		
20.24	Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления информационной системой*		
20.25	Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и средствами защиты информации*		
20.26	Угроза подмены сетевых адресов, определяемых по сетевым именам*		
20.27	Угроза отсутствия проверки подлинности сетевых соединений*		
20.28	Отсутствие подтверждения факта отправки/получения информации конкретными пользователями*		
20.29	Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами		
20.30	Отсутствие контроля соединений между СВТ ИС		
20.31	Угроза несанкционированного доступа к средствам управления информационными потоками		
20.32	Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации		
20.33	Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения		
20.34	Угроза доступа к ИС с использованием беспроводного доступа из-за границ КЗ		

1	2	3	4
21	**Угрозы инженерной инфраструктуре**		
21.1	Угрозы сбоев в сети электропитания		
21.2	Угроза выхода из строя ТС в результате нарушения климатических параметров работы		
21.3	Угрозы нарушения схем электропитания*		
21.4	Угрозы, связанные с отсутствием заземления/неправильным заземлением *		
22.	**Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности**		
22.1	Угроза отсутствия системы регистрации событий информационной безопасности*		
22.2	Угроза автоматического удаления/затирания событий информационной безопасности новыми события*		
22.3	Угроза переполнения журналов информационной безопасности*		
22.4	Угроза отсутствия централизованной подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, средств защиты информации*		
22.5	Угроза неправильного отнесения событий к событиям информационной безопасности*		
22.6	Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств защиты информации*		
22.7	Угроза отключения журналов информационной безопасности*		
22.8	Угроза модификации/удаления журнала информационной безопасности*		
22.9	Угроза задержек при получении журналов информационной безопасности		

1	2	3	4
22.10	Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени		
22.11	Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности*		
22.12	Угроза отключения/отказа системы регистрации событий информационной безопасности		
22.13	Угроза несанкционированного изменения правил ведения журнала регистрации событий		
22.14	Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности		
23.	**Угрозы, связанные с контролем защищенности информационной системы**		
23.1	Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения *		
23.2	Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности*		
23.3	Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей		
23.4	Угроза отсутствия регулярного контроля за защищенностью информационной системы, в том числе средств защиты информации с учетом новых угроз безопасности информации		
23.5	Угроза отсутствия анализа изменения настроек информационной системы, компонентов информационной системы, в том числе средств защиты информации на предмет появления уязвимостей*		
23.6	Отсутствие журнала анализа защищенности		

1	2	3	4
24.	**Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи**		
24.1	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевой трафик
24.2	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение
24.3	Угроза перехвата данных *		
24.4	Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена		
24.5	Угроза перехвата данных с сетевых портов		
24.6	Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа*		

Примечание:
* – базовые УБ ПДн в ИСПДн.
Незаполненные ячейки вышеприведенной таблицы определяются в частных моделях угроз и нарушителя безопасности информации для каждой ИСПДн.

Приложение № 2
«Актуальные угрозы безопасности персональных данных при обработке в информационных системах персональных данных»

ТИПОВЫЕ ВОЗМОЖНОСТИ
нарушителей безопасности информации и направления атак

№ п/п	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия (при наличии)
1	2	3	4
1	Проведение атаки при нахождении за пределами контролируемой зоны		
2	Проведение атаки при нахождении в пределах контролируемой зоны		
3	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ		
4	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ		
5	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ		
6	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		

1	2	3	4
7	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО		
8	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
9	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		
10	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО		
11	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ		
12	Возможность воздействовать на любые компоненты СКЗИ и СФ		

Примечание: незаполненные ячейки вышеуказанной таблицы определяются в частных моделях угроз и нарушителя безопасности информации для каждой ИСПДн.