КАБИНЕТ МИНИСТРОВ
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
МИНИСТРЛАР КАБИНЕТЫ

РАСПОРЯЖЕНИЕ **БОЕРЫК**

29.12.2018 г.Казань № 3768-р

В целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов государственной власти Республики Татарстан и органов местного самоуправления муниципальных районов и городских округов Республики Татарстан, с учетом положений части 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Утвердить прилагаемое Положение об определении актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных Республики Татарстан (далее – Положение).

2. Исполнительным органам государственной власти Республики Татарстан и подведомственным им организациям при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых информационных системах персональных данных, руководствоваться Положением.

3. Рекомендовать государственным органам Республики Татарстан, не являющимся исполнительными органами государственной власти Республики Татарстан, органам местного самоуправления муниципальных районов и городских округов Республики Татарстан, подведомственным им организациям, а также организациям, в уставном (складочном) капитале которых доля (вклад) Республики Татарстан и (или) муниципальных образований Республики Татарстан составляет 50 процентов и более и расположенным на территории Республики Татарстан, при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых информационных системах персональных данных, руководствоваться Положением.

4. Контроль за исполнением настоящего распоряжения возложить на Министерство информатизации и связи Республики Татарстан.

Премьер-министр
Республики Татарстан А.В.Песошин

Утверждено
распоряжением
Кабинета Министров
Республики Татарстан
от 29.12.2018 № 3768-р

Положение
об определении актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных Республики Татарстан

1. Общие положения

1.1. Настоящее Положение определяет перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами государственной власти Республики Татарстан (далее – Органы), при осуществлении ими соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. Указанный перечень уточняется по мере выявления новых угроз безопасности персональных данных и их источников, развития способов и средств их реализации.

1.2. Настоящее Положение не регулирует отношения, связанные с обеспечением безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.3. Настоящее Положение применяется Органами при решении ими следующих задач:

определение угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных;

анализ защищенности информационных систем персональных данных от актуальных угроз безопасности персональных данных в ходе выполнения мероприятий по информационной безопасности (защите информации);

модернизация системы защиты персональных данных в Органах;

проведение мероприятий по минимизации и (или) нейтрализации угроз безопасности персональных данных;

предотвращение несанкционированного воздействия на технические средства информационных систем персональных данных;

контроль за обеспечением уровня защищенности персональных данных.

1.4. При определении актуальных угроз безопасности персональных данных Органы разрабатывают модели угроз безопасности персональных данных для эксплуатируемых ими информационных систем персональных данных с учетом содержания персональных данных, характера и способов их обработки, условий и особенностей функционирования информационных систем персональных данных и

совокупности условий и факторов, создающих актуальную опасность несанкционированного доступа к персональным данным, и применяют:

группы актуальных угроз безопасности персональных данных в информационных системах персональных данных, приведенные в разделе 6 настоящего Положения;

расширенный перечень угроз безопасности персональных данных в информационных системах персональных данных, приведенный в приложении № 1 к настоящему Положению;

типовые возможности нарушителей безопасности информации и направления атак, приведенные в приложении № 2 к настоящему Положению.

1.5. При определении актуальных угроз безопасности персональных данных в информационных системах персональных данных Органы руководствуются положениями следующих нормативных правовых актов:

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

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

постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»;

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

приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

приказ Федеральной службы по техническому и экспортному контролю 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 Федеральной службы безопасности Российской Федерации 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»;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 года;

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю от 15 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, разработанные Министерством здравоохранения и социального развития Российской Федерации, согласованные с Федеральной службой по техническому и экспортному контролю 22 декабря 2009 года;

Модель угроз типовой медицинской информационной системы типового лечебного профилактического учреждения, разработанная Министерством здравоохранения и социального развития Российской Федерации, согласованная с Федеральной службой по техническому и экспортному контролю 27 ноября 2009 года;

Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, согласованная с Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и одобренная решением секции № 1 Научно-технического совета Министерства связи и массовых коммуникаций Российской Федерации «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2;

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя 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 Государственной технической комиссии при Президенте Российской Федерации № 7.2/02.03.01 г.;

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 Федеральной службы безопасности Российской Федерации (от 31 марта 2015 года № 149/7/2/6-432).

1.6. В настоящем Положении 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 г. № 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 Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 года.

В настоящем Положении применяются следующие сокращения:

АРМ – автоматизированное рабочее место;

ГИСТ РТ – Государственная интегрированная система телекоммуникаций Республики Татарстан;

ИСПДн – информационная система персональных данных;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина (АРМ);

реестр – стандартный реестр операционной системы;

ТС – технические средства.

2. Владельцы и операторы информационных систем персональных данных, сети передачи данных

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

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

2.3. Контролируемой зоной ИСПДн, функционирующих в Органах, являются здания и отдельные помещения, принадлежащие им или арендуемые этими Органами. Все средства вычислительной техники, участвующие в обработке персональных данных, располагаются в пределах контролируемой зоны Органа. 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.

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

внешним сетям (сетям провайдера), подключение к которым организовано посредством проводных (медных и оптоволоконных) каналов связи операторов связи (провайдеров);

сетям Органов, организаций, расположенных на территории Российской Федерации. Подключение к указанным сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Органы исполнительной власти Республики Татарстан имеют подключение к ГИСТ РТ посредством защищенных каналов связи;

иным сетям, взаимодействие с которыми организовано Органами с целью исполнения своих полномочий.

2.5. Подключение к сетям связи общего пользования осуществляется Органами 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 персональных данных в информационных системах персональных данных

3.1. При определении Органами угрозы безопасности персональным данным в конкретной ИСПДн защите подлежат следующие объекты, входящие в ИСПДн:

персональные данные, обрабатываемые в ИСПДн;

информационные ресурсы ИСПДн (файлы, базы данных и т.п.);

средства вычислительной техники, участвующие в обработке персональных данных посредством ИСПДн;

средства криптографической защиты информации и средства защиты информации;

среда функционирования средств криптографической защиты информации;

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию средств криптографической защиты информации;

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 средства криптографической защиты информации и на технические и программные компоненты среды функционирования средств криптографической защиты информации;

носители защищаемой информации, используемые в ИСПДн, в том числе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации средств криптографической защиты информации 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 персональные данные посредством ИСПДн и располагаются компоненты ИСПДн;

помещения, в которых находятся ресурсы ИСПДн, имеющие отношение к криптографической защите персональных данных.

3.2. В состав средств вычислительной техники, участвующих в обработке персональных данных посредством ИСПДн, входят:

АРМ пользователей с различными уровнями доступа (правами);

терминальная станция;

серверное оборудование;

сетевое и телекоммуникационное оборудование;

общесистемное ПО (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.).

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

4. Информационные системы персональных данных

4.1. В целях исполнения своих полномочий Органами обрабатываются все категории персональных данных. Состав персональных данных, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции), совершаемые с персональными данными в ИСПДн, определяются Органом, являющимся оператором ИСПДн.

4.2. Обработка персональных данных в ИСПДн осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Перечень обрабатываемых персональных данных в ИСПДн должен соответствовать целям их обработки.

4.3. ИСПДн подразделяются на:

ИСПДн, оператором которых является сам Орган;

ИСПДн, эксплуатируемые Органом, не в качестве ее оператора.

4.4. ИСПДн и ее компоненты должны быть расположены в Российской Федерации.

4.5. ИСПДн подразделяются в зависимости от технологии обработки персональных данных, целей и состава персональных данных на следующие категории:

информационно-справочные;

сегментные;

республиканские;

ведомственные;

служебные.

Для всех категорий персональных данных вышеуказанных категорий ИСПДн необходимо обеспечивать следующие характеристики безопасности: конфиденциальность, целостность, доступность. В рамках ИСПДн возможна модификация и передача персональных данных.

4.5.1. Информационно-справочные ИСПДн используются в целях официального доведения любой информации до определенного или неопределенного круга лиц.

К информационно-справочным ИСПДн относятся:

официальные порталы (сайты) Органов;

информационные порталы (сайты), которые ведутся Органом в целях реализации проекта и (или) проведения мероприятия на территории Республики Татарстан (далее – информационные порталы (сайты));

закрытые порталы для нескольких групп участников Органов;

Портал государственных и муниципальных услуг Республики Татарстан.

4.5.1.1. Официальные порталы (сайты) Органов содержат сведения о деятельности Органов, в том числе сведения, подлежащие обязательному размещению в указанных ИСПДн в соответствии с законодательством.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками Органа, являющегося оператором ИСПДн, гражданами Российской Федерации и других государств. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

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

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.2. Информационные порталы (сайты) содержат сведения о мероприятиях, проводимых Органами в соответствии с их функциями и полномочиями.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется посредством веб-интерфейса сотрудниками Органа, являющегося оператором ИСПДн, гражданами Российской Федерации и других государств. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

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

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.3. Закрытые порталы для нескольких групп участников Органов содержат сведения, предоставляемые ограниченному кругу лиц из числа Органов в соответствии с их функциями и полномочиями.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Органов посредством веб-интерфейса в соответствии с предоставленными правами. Персональные данные хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органов.

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

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.1.4. Портал государственных и муниципальных услуг Республики Татарстан содержит социально значимую информацию и сведения, необходимые для получения гражданами государственных и муниципальных услуг в электронном виде.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Органов, гражданами Российской Федерации и других государств посредством веб-интерфейса.

Персональные данные обрабатываются в деперсонифицированном (обезличенном) виде. Запрашиваемые данные не позволяют однозначно идентифицировать субъекта персональных данных без использования сторонних баз данных. После получения запрашиваемых данных ИСПДн в целях получения ответа на запрос субъекта персональных данных передает его данные по закрытым каналам связи в

ИСПДн иных Органов, в чью компетенцию входит предоставление информации по запросу субъекта. Ответ на запрос (сведения о ходе исполнения запроса) субъекта отображается в указанной ИСПДн.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

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

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.2. Сегментные ИСПДн представляют собой сегменты федеральных информационных систем, создаются и эксплуатируются в Республике Татарстан на основании предоставляемых оператором федеральной информационной системы рекомендаций (правовых, организационных, технических) и используются для сбора, обработки, свода данных в Республике Татарстан и передачи их оператору федеральной информационной системы, и наоборот, при этом цели и задачи создания (модернизации), эксплуатации данных информационной системы определяются оператором федеральной информационной системы. Данные ИСПДн предназначены для реализации полномочий федеральных органов власти и исполнения функций Органов.

Обработке в ИСПДн могут подлежать все категории персональных данных.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Органов в специализированных программах и (или) посредством веб-интерфейса, а в отдельных случаях – гражданами Российской Федерации и других государств в режиме веб-интерфейса (с ограниченными правами доступа).

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Органа.

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными 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 персональных данных осуществляется с использованием машинных носителей);

посредством ГИСТ РТ;

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

Средства вычислительной техники, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

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 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, 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 6 апреля 2011 года № 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 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

4.5.3. Республиканские ИСПДн создаются и эксплуатируются по желанию (на основании решения) Республики Татарстан или Органа в интересах нескольких Органов, при этом цели и задачи создания (модернизации), эксплуатации данных ИСПДн, а также требования к ним определяются Республикой Татарстан или Органом соответственно.

По выполняемым функциям республиканские ИСПДн подразделяются на:

интеграционные;

многопрофильные;

ИСПДн для Органов и организаций Республики Татарстан.

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

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

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

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа.

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством ГИСТ РТ;

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

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.3.2. ИСПДн многопрофильные предназначены для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам в Органах.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Органов в специализированных программах в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: граждане Российской Федерации и других государств.

Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа.

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

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

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

посредством ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

4.5.3.3. ИСПДн для Органов и организаций Республики Татарстан предназначены для автоматизации совместной деятельности Органов и организаций Республики Татарстан, в том числе деятельности, которая необходима к исполнению в соответствии с требованиями законодательства.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется в соответствии с предоставленными правами сотрудниками Органов и организаций Республики Татарстан в специализированных программах в режиме веб-интерфейса.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органов и организаций Республики Татарстан.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

По архитектуре республиканские ИСПДн подразделяются на:

сегментированные;

централизованные;

смешанные.

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, выполняющее 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 сегментированные 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 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 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 6 апреля 2011 года № 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 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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, являющиеся 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 централизованные 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 6 апреля 2011 года № 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 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

4.5.4. Ведомственные ИСПДн создаются (эксплуатируются) по решению Органа в своих интересах, цели и задачи создания (модернизации), эксплуатации которых определяются Органом. Ведомственные ИСПДн предназначены для исполнения функций Органов.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

специальные;

иные.

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

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники оператора ИСПДн и иных Органов, а также сторонние граждане.

Структура ИСПДн: распределенная или локальная, функционирующая в контролируемой зоне Органа.

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

ИСПДн без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Обмен (передача и получение) персональными данными 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 персональных данных осуществляется с использованием машинных носителей);

посредством ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Также обмен персональными данными между сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется посредством собственных корпоративных сетей Органа.

Средства вычислительной техники, участвующие в обработке: АРМ, терминальная станция, серверное оборудование, сетевое и телекоммуникационное оборудование.

По архитектуре ведомственные ИСПДн подразделяются на:

сегментированные;

централизованные;

смешанные.

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, выполняющее 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 сегментированные 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 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 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 6 апреля 2011 года № 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 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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, являющиеся 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 централизованные 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 6 апреля 2011 года № 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 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

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

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

К основным служебным ИСПДн относятся:

ИСПДн бухгалтерского учета и управления финансами;

ИСПДн кадрового учета и управления персоналом;

ИСПДн документооборота и делопроизводства;

ИСПДн поддерживающие.

4.5.5.1. ИСПДн бухгалтерского учета и управления финансами предназначены для автоматизации деятельности Органа, связанной с ведением бухгалтерского учета и управлением финансами.

Обработке в ИСПДн подлежат иные категории персональных данных.

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

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

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 или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа;

построенные по технологии «тонкого клиента»: на рабочие места пользователей ИСПДн передается только графическая информация, сама обработка данных осуществляется на удаленном серверном сегменте (сервере или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа.

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

4.5.5.2. ИСПДн кадрового учета и управления персоналом предназначены для автоматизации деятельности Органа, связанной с ведением кадрового учета и управления персоналом.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

специальные;

иные.

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

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

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа.

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

ИСПДн без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных 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 или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа. Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.3. ИСПДн документооборота и делопроизводства предназначены для автоматизации деятельности Органа, связанной с осуществлением документооборота и делопроизводства.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки персональных данных в ИСПДн: многопользовательский. ИСПДн предусматривает разграничение доступа. Обработка персональных данных осуществляется сотрудниками Органов в специализированных программах в соответствии с предоставленными правами.

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные с использованием иных каналов связи.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

посредством ГИСТ РТ;

с использованием сторонних средств криптографической защиты информации.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

Технология обработки персональных данных 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 или АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа. Доступ к персональным данным в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора).

4.5.5.4. ИСПДн поддерживающие. Предназначены для автоматизации деятельности Органа, связанной с осуществлением им (его сотрудниками) своих функций, полномочий и задач.

Категории персональных данных, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

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

Типы субъектов персональных данных, которые могут подлежать обработке в ИСПДн: сотрудники Органа, являющегося оператором ИСПДн, граждане Российской Федерации и других государств.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа.

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

без подключения (передача персональных данных осуществляется с использованием машинных носителей);

подключенные посредством ГИСТ РТ;

подключенные с использованием иных каналов связи.

Передача персональных данных в иные ИСПДн не осуществляется.

Средства вычислительной техники, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование.

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 или АРМ, выполняющему функцию сервера), располагающемуся в пределах контролируемой зоны Органа;

построенные на базе стандартного офисного ПО: 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.

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

5. Угрозы безопасности персональных данных, выявленные при функционировании информационной системы персональных данных

5.1. Источниками угрозы безопасности персональных данных выступают:

носитель вредоносной программы;

аппаратная закладка;

нарушитель.

5.1.1. 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.), флеш-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, с файлами, имеющими определенные расширения или иные атрибуты, с 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 (персональных данных):

аппаратная закладка внутри клавиатуры;

считывание данных с кабеля клавиатуры бесконтактным методом;

включение устройства в разрыв кабеля;

аппаратная закладка внутри системного блока и др.

Ввиду отсутствия возможности неконтролируемого пребывания физических лиц в служебных помещениях, в которых размещены технические средства ИСПДн, или в непосредственной близости от них, соответственно исключается вероятность установки аппаратных закладок посторонними лицами.

5.1.3. Нарушитель. Под нарушителем безопасности информации понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием

которых является нарушение безопасности персональных данных при их обработке в ИСПДн.

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

внешний нарушитель. Указанный тип нарушителя не имеет права постоянного или имеет право разового (контролируемого) доступа в контролируемую зону, также не имеет доступа к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны, или он ограничен и контролируется. Указанный тип нарушителя может реализовывать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренний нарушитель, имеющий доступ к ИСПДн. Указанный тип нарушителя имеет право постоянного (периодического) доступа на территорию контролируемой зоны, а также доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Указанный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн;

внутренний нарушитель, не имеющий доступа к ИСПДн. Указанный тип нарушителя имеет право постоянного (периодического) доступа на территорию контролируемой зоны, но не имеет доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Указанный тип нарушителя может проводить атаки с использованием внутренней (локальной) сети передачи данных.

5.2. Основными угрозами безопасности персональных данных в ИСПДн являются:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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 угрозы безопасности персональных данных в информационных системах персональных данных

6.1. В настоящем разделе приведены группы актуальных угроз безопасности персональных данных в ИСПДн из групп, указанных в пункте 5.2 настоящего Положения, исходя из содержания персональных данных, характера и способов их обработки.

6.2. Информационно-справочные ИСПДн:

6.2.1. Официальные порталы (сайты) Органов:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Информационные порталы (сайты):

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Закрытые порталы для нескольких групп участников Органов:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Портал государственных и муниципальных услуг Республики Татарстан:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Сегментные ИСПДн:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Республиканские ИСПДн:

6.4.1. ИСПДн интеграционные:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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 несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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 и организаций Республики Татарстан:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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. Ведомственные ИСПДн:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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.

6.6. Служебные ИСПДн:

6.6.1. ИСПДн бухгалтерского учета и управления финансами:

грозы утечки информации по техническим каналам;

грозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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.

6.6.2. ИСПДн кадрового учета и управления персоналом:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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.

6.6.3. ИСПДн документооборота и делопроизводства:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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.

6.6.4. ИСПДн поддерживающие:

угрозы утечки информации по техническим каналам;

угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы недекларированных возможностей в системном ПО и прикладном ПО;

угрозы, не являющиеся атаками;

угрозы несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа в результате нарушения процедуры авторизации и аутентификации;

угрозы несанкционированного доступа 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 ПО и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, 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.

Приложение № 1
к Положению об определении
актуальных угроз безопасности
персональных данных при их
обработке в информационных
системах персональных данных
Республики Татарстан

Расширенный перечень
угроз безопасности персональных данных в информационных системах персональных данных

№ п/п	Наименование угрозы безопасности персональных данных в ИСПДн*	Источники угрозы безопасности персональных данных	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		
1.1.2.	Использование «контактных микрофонов» для съема виброакустических сигналов		
1.1.3.	Использование «лазерных микрофонов» для съема виброакустических сигналов		
1.1.4.	Использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет «микрофонного эффекта» в технических средствах обработки информации и		

*Список использованных сокращений – на стр.40.

1	2	3	4
	вспомогательных технических средствах и системах (распространяются по проводам и линиям, выходящим за пределы служебных помещений)		
1.1.5.	Применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении технических средств обработки информации и вспомогательных технических средств и систем ВЧ-сигналом		
1.1.6.	Применение акустооптических модуляторов на базе волоконно-оптической связи, находящихся в поле акустического сигнала («оптических микрофонов»)		
1.2.	Угрозы утечки видовой информации		
1.2.1.	Визуальный просмотр на экранах дисплеев и других средств отображения средств вычислительной техники, измерительно-вычислительного комплекса, входящих в состав информационных систем		
1.2.2.	Визуальный просмотр с помощью оптических (оптико-электронных) средств на экранах дисплеев и других средств отображения средств вычислительной техники, измерительно-вычислительного комплекса, входящих в состав информационной системы		
1.2.3.	Использование специальных электронных устройств съема видовой информации (видеозакладки)		
1.3.	Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок		
1.3.1.	Применение специальных средств регистрации побочных электромагнитных излучений и наводок от ТС и линий передачи информации (программно-аппаратный комплекс, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)		

1	2	3	4
1.3.2.	Применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящих за пределы служебных помещений		
1.3.3.	Применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС информационной системы, или при наличии паразитной генерации в узлах ТС		
1.3.4.	Применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС информационной системы, в которых проводится обработка информативных сигналов – параметрических каналов утечки		
2.	Угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа к информации		
2.1.	Угроза некорректного использования функционала ПО	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, 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 ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр
2.3.	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, объекты файловой системы, учетные 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

1	2	3	4
2.5.	Доступ в операционную среду (локальную операционную систему отдельного ТС информационной системы) с возможностью выполнения несанкционированного доступа, 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 ПО, сетевое ПО, 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
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 ПО, сетевое ПО, сетевой трафик

1	2	3	4
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 ПО, сетевое ПО
3.10.	Угроза утраты вычислительных ресурсов	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное ПО, сетевое ПО, сетевой трафик
3.11.	Угроза вывода/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**		
3.14.	Угроза потери информации в процессе ее обработки техническими 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 информационной системы 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**		

**Базовые угрозы безопасности персональных данных в ИСПДн.

1	2	3	4
4.	Угрозы нарушения целостности информации		
4.1.	Угроза нарушения целостности данных кеша	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Сетевое ПО
4.2.	Угроза некорректного задания структуры данных транзакции	Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое ПО
4.3.	Угроза переполнения целочисленных переменных	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО
4.4.	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель с низким потенциалом	Прикладное ПО, сетевое ПО, 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 измененных файлов	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное ПО
4.7.	Угроза отсутствия контроля целостности обрабатываемой в информационной системе информации, применяемого ПО, в том числе в средствах защиты информации**		
4.8.	Угроза отсутствия целостных резервных копий информации, ПО, 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		

1	2	3	4
4.11.	Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в информационную систему информации		
4.12.	Угроза доступа в информационную систему информации от неаутентифицированных серверов/пользователей		
4.13.	Угроза отсутствия контроля за данными, передаваемыми из информационной системы**		
4.14.	Отсутствие резервного копирования информации, передаваемой из информационной системы		
4.15.	Угроза передачи из информационной системы 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 ПО, прикладного ПО, средств защиты**		
4.20.	Угроза установки/запуска модифицированного ПО и (или) модифицированных обновлений ПО		
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 информационной системой, и ее структуры		

1	2	3	4
5.	Угрозы недекларированных возможностей в системном ПО и прикладном ПО		
5.1.	Угроза перебора всех настроек и параметров приложения		
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 информационной системе		
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 ПО, 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 несанкционированного доступа, создающие предпосылки для реализации несанкционированного доступа 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 ПО, метаданные, учетные данные пользователя
7.3.	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, сетевое ПО
7.4.	Угроза программного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное ПО
7.5.	Угроза «кражи» учетной записи доступа к сетевым сервисам	Внешний нарушитель с низким потенциалом	Сетевое ПО
7.6.	Угроза получения доступа к информационной системе, компонентам информационной системы, информации, обрабатываемой информационной системой без прохождения процедуры идентификации и аутентификации**		
7.7.	Угроза получения доступа к информационной системе 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 информационной системы		
7.11.	Угрозы авторизации с использованием устаревших, но не отключенных учетных записей**		

1	2	3	4
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 информационной системе посредством удаленного доступа		
7.15.	Угроза передачи аутентифицирующей информации по открытым каналам связи без использования средств криптографической защиты информации		
7.16.	Угроза доступа к информационной системе 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		

1	2	3	4
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, ПО телекоммуникационного оборудования		
8.	Угрозы несанкционированного доступа 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 ПО, 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 ПО
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 ПО, прикладное ПО, сетевое ПО
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 ПО, системное ПО

1	2	3	4
8.8.	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	Внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом	Средства защиты информации, системное ПО, сетевое ПО, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты
8.9.	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО
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 счет плагинов браузера	Внешний нарушитель с низким потенциалом	Сетевое ПО
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 ПО, объекты файловой системы, учетные данные пользователя, реестр, машинные носители информации
8.15.	Угроза несанкционированного доступа к системе по беспроводным каналам	Внешний нарушитель с низким потенциалом	Сетевой узел, учетные 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

1	2	3	4
8.17.	Угроза несанкционированного редактирования реестра	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, использующее реестр, реестр
8.18.	Угроза несанкционированного создания учетной записи пользователя	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО
8.19.	Угроза несанкционированного управления буфером	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО
8.20.	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение
8.21.	Угроза несанкционированного управления указателями	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО
8.22.	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	Внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО
8.23.	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, аппаратное обеспечение
8.24.	Угроза перехвата привилегированного потока	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО
8.25.	Угроза перехвата привилегированного процесса	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО
8.26.	Угроза повышения привилегий	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, сетевое ПО, 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 ПО
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 ПО, микропрограммное обеспечение, учетные данные пользователя
8.31.	Угроза «форсированного веб-браузинга»	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО
8.32.	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО
8.33.	Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой операционной системы 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 информационной системы, так и между информационными системами **		

1	2	3	4
8.37.	Угроза получения дополнительных данных, не предусмотренных технологией обработки**		
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 информационной системы, 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 информационной системы до прохождения процедур идентификации и авторизации**		
8.43.	Угрозы несанкционированного подключения к информационной системе с использованием санкционированной сессии удаленного доступа**		
8.44.	Угроза подбора идентификационных данных для удаленного доступа к информационной системе**		
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 информационной системе с использованием технологий беспроводного доступа, в том числе с мобильных устройств, без прохождения процедуры идентификации и авторизации**		

1	2	3	4
8.48.	Угроза получения доступа к информационной системе с использованием технологий беспроводного доступа, с неконтролируемых устройств**		
8.49.	Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем**		
8.50.	Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации**		
8.51.	Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей**		
8.52.	Угроза бесконтрольного доступа к информации неопределенного круга лиц**		
8.53.	Угроза получения доступа к данным, не предназначенным для пользователя**		
8.54.	Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей**		
8.55.	Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами**		
8.56.	Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к информационной системе при использовании в информационной системе мобильных устройств**		
8.57.	Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты		

1	2	3	4
8.58.	Отсутствие отказоустойчивых централизованных средств управления учетными записями		
8.59.	Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к информационной системе, выявления попыток несанкционированного доступа		
8.60.	Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации		
8.61.	Угроза передачи информации разной степени конфиденциальности без разграничения информационных потоков		
8.62.	Угроза передачи информации без соблюдения атрибутов (меток) безопасности, связанных с передаваемой информацией		
8.63.	Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния информационной системы, условий ее функционирования, изменений в технологии обработки передаваемых данных		
8.64.	Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными		
8.65.	Угроза несанкционированного доступа к средствам управления информационными потоками		
8.66.	Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо		
8.67.	Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним		

1	2	3	4
8.68.	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 информационной системе, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа		
8.69.	Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями		
8.70.	Угроза использования одних и тех же учетных записей для параллельного доступа к информационной системе (с двух и более) различных устройств		
8.71.	Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия 5 минут		
8.72.	Угроза использования незавершенных сеансов пользователей		
8.73.	Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования информационной системы, системы защиты, в том числе с использованием технологий беспроводного доступа		
8.74.	Отсутствие автоматизированного мониторинга и контроля удаленного доступа		
8.75.	Угроза использования уязвимых/незащищенных технологий удаленного доступа		
8.76.	Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты		

1	2	3	4
8.77.	Отсутствие механизмов автоматизированного контроля параметров настройки компонентов ПО, влияющих на безопасность информации		
8.78.	Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов ПО, влияющих на безопасность информации		
8.79.	Отсутствие контроля за используемыми интерфейсами ввода/вывода		
9.	Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн		
9.1.	Угроза передачи данных по скрытым каналам	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
9.2.	Угроза включения в проект не испытанных достоверно компонентов	Внутренний нарушитель со средним потенциалом	ПО, техническое средство, информационная система, ключевая система информационной инфраструктуры
9.3.	Угроза внедрения системной избыточности	Внутренний нарушитель со средним потенциалом	ПО, 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 путем обмана	Внешний нарушитель со средним потенциалом	Прикладное ПО, сетевое ПО

1	2	3	4
10.2.	Угроза «фишинга»	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое ПО, сетевой трафик
10.3.	Реализация угроз с использованием возможности непосредственного доступа к техническим и части программных средств информационной системы, средствам защиты информации и средствам криптографической защиты информации 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 информационной системы/модулей/компонентов/сегментов ЕСЭДД, средств защиты информации (в случае сговора с внешними нарушителями безопасности информации)**		
10.5.	Создание неконтролируемых точек доступа (лазеек) в систему для удаленного доступа к информационной системе**		
10.6.	Переконфигурирование средств защиты информации и средств криптографической защиты информации для реализации угроз информационной системе**		
10.7.	Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления**		
10.8.	Хищение ключей шифрования, идентификаторов и известных паролей**		
10.9.	Внесение программно-аппаратных закладок в программно-аппаратные средства информационной системы, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации**		

1	2	3	4
10.10.	Создание методов и средств реализации атак, а также самостоятельное проведение атаки		
10.11.	Ошибки при конфигурировании и обслуживании модулей/компонентов информационной системы		
10.12.	Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация ПО; 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 персональных данных 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 ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение
11.2.	Угроза исследования приложения через отчеты об ошибках	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение

1	2	3	4
11.3.	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
11.4.	Угроза обнаружения хостов	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
11.5.	Угроза определения типов объектов защиты	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
11.6.	Угроза определения топологии вычислительной сети	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
11.7.	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое ПО, сетевой трафик, прикладное ПО
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 ПО, сетевой узел
11.10.	Сканирование сети для изучения логики работы информационной системы, выявления протоколов, портов**		
11.11.	Анализ сетевого трафика для изучения логики работы информационной системы, 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 информационной системы и ее системе защиты		
11.14.	Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в информационной системе		
11.15.	Угроза получения нарушителем идентификационных данных легальных пользователей информационной системы		

1	2	3	4
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 ПО, прикладное ПО, сетевое ПО
12.3.	Угроза восстановления аутентификационной информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, микропрограммное обеспечение, учетные данные пользователя
12.4.	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО, 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 ПО, сетевое ПО
12.6.	Угроза искажения XML-схемы	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое ПО, сетевой трафик
12.7.	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО, аппаратное обеспечение
12.8.	Угроза использования слабостей кодирования входных данных	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр
12.9.	Угроза межсайтового скриптинга	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО
12.10.	Угроза межсайтовой подделки запроса	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое ПО

1	2	3	4
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 ПО, прикладное ПО, аппаратное обеспечение
12.13.	Угроза подмены резервной копии ПО BIOS	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI
12.14.	Угроза пропуска проверки целостности ПО	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО
12.15.	Угроза заражения компьютера при посещении неблагонадежных сайтов	Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО
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 ПО
12.18.	Угроза распространения «почтовых червей»	Внешний нарушитель с низким потенциалом	Сетевое ПО
12.19.	Внедрение программных закладок/закладок**		
12.20.	Угроза внедрения в информационную систему вредоносного ПО с устройств, подключаемых с использованием технологий беспроводного доступа**		
12.21.	Применение специально созданных программных продуктов для несанкционированного доступа**		
12.22.	Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного ПО**		
12.23.	Отсутствие централизованной системы управления средствами антивирусной защиты		

1	2	3	4
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 обеспечения и ПО	Внешний нарушитель с низким потенциалом	Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное ПО
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 незащищенного администрирования облачных услуг	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Облачная система, рабочая станция, сетевое ПО
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

1	2	3	4
13.10.	Угроза некорректной реализации политики лицензирования в облаке	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, прикладное ПО, сетевое ПО
13.11.	Угроза неопределенности в распределении ответственности между ролями в облаке	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО
13.12.	Угроза неопределенности 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 политики безопасности элементов облачной инфраструктуры	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, 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 ПО, метаданные, объекты файловой системы
13.18.	Угроза потери управления облачными ресурсами	Внешний нарушитель с высоким потенциалом	Сетевой трафик, объекты файловой системы
13.19.	Угроза потери управления собственной инфраструктурой при переносе ее в облако	Внутренний нарушитель со средним потенциалом	Информационная система, иммигрированная в облако, системное ПО, прикладное ПО, сетевое ПО

1	2	3	4
13.20.	Угроза привязки к поставщику облачных услуг	Внутренний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, системное ПО, сетевое ПО, сетевой трафик, объекты файловой системы
13.21.	Угроза приостановки оказания облачных услуг вследствие технических сбоев		Системное ПО, 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 ПО
14.4.	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера
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, учетные данные пользователя, образ виртуальной машины

1	2	3	4
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 путем несанкционированного внесения изменений в образы виртуальных машин	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Образ виртуальной машины, сетевой узел, сетевое ПО, 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 ПО, 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
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

1	2	3	4
15.12.	Угроза ошибки обновления гипервизора	Внутренний нарушитель с низким потенциалом	Системное ПО, гипервизор
15.13.	Угроза перехвата управления гипервизором	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Системное ПО, гипервизор, консоль управления гипервизором
15.14.	Угроза перехвата управления средой виртуализации	Внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	Информационная система, системное ПО
15.15.	Нарушение доверенной загрузки виртуальных серверов информационной системы, 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 информационной системы, в том числе несанкционированное сетевое подключение и проведение сетевых атак на виртуальный сервер информационной системы**		
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**		

1	2	3	4
15.22.	Угроза отсутствия средств регистрации событий в виртуальной инфраструктуре**		
16.	Угрозы, связанные с нарушением правил эксплуатации машинных носителей		
16.1.	Угроза несанкционированного восстановления удаленной 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 информационной системе неучтенных машинных носителей**		
16.8.	Угроза подключения к информационной системе неперсонифицированных машинных носителей		
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**		

1	2	3	4
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 портов средств вычислительной техники 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 контролируемой зоны		
17.	Угрозы, связанные с нарушением процедур установки/обновления ПО 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 ПО, прикладное ПО, 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 ПО и (или) обновлений ПО**		
17.6.	Установка ПО, содержащего известные уязвимости**		
17.7.	Установка нелицензионного ПО**		
17.8.	Угроза ошибочного запуска/установки ПО**		
17.9.	Угроза неправильной установки ПО**		
17.10.	Угроза автоматического запуска вредоносного/шпионского/ неразрешенного ПО при запуске операционной системы и (или) обновлений ПО		
17.11.	Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного ПО		
17.12.	Угроза несанкционированного запуска ПО в нерабочее время		
18.	Угрозы физического доступа к компонентам ИСПДн		
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 накопителя на жестких магнитных дисках 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 контролируемую зону**		
18.9.	Отсутствие средств автоматизированного контроля доступа		
19.	Угрозы эксплуатации уязвимостей в системном ПО, прикладном ПО, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах ИСПДн, микропрограммном обеспечении		
19.1.	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное ПО
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 ПО, 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 ПО

1	2	3	4
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 ПО
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 ПО 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 ПО
19.14.	Угроза наличия механизмов разработчика	Внутренний нарушитель со средним потенциалом	ПО, техническое средство
19.15.	Угроза спама веб-сервера	Внешний нарушитель с низким потенциалом	Сетевое ПО
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 ПО, сетевой трафик
20.3.	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Системное ПО, сетевое ПО, сетевой трафик

1	2	3	4
20.4.	Угроза неправомерных действий в каналах связи	Внешний нарушитель с низким потенциалом	Сетевой трафик
20.5.	Угроза несанкционированного удаленного 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 ПО
20.7.	Угроза подмены беспроводного клиента или точки доступа	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО, аппаратное обеспечение, точка беспроводного доступа
20.8.	Угроза подмены доверенного пользователя	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое ПО
20.9.	Угроза подмены субъекта сетевого доступа	Внешний нарушитель со средним потенциалом	Прикладное ПО, сетевое ПО, сетевой трафик
20.10.	Угроза «фарминга»	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое ПО, 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 информационную систему 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**		

1	2	3	4
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**		
20.22.	Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств**		
20.23.	Угроза подмены устройств, подключаемых к информационной системе 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		

1	2	3	4
20.30.	Отсутствие контроля соединений между средствами вычислительной техники информационной системы		
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 ПО		
20.34.	Угроза доступа к информационной системе с использованием беспроводного доступа из-за границ контролируемой зоны		
21.	Угрозы инженерной инфраструктуры		
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 событиями**		
22.3.	Угроза переполнения журналов информационной безопасности**		

1	2	3	4
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		
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		

1	2	3	4
22.14.	Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности		
23.	Угрозы, связанные с контролем защищенности ИСПДн		
23.1.	Угроза отсутствия контроля за уязвимостями информационной системы, компонентов информационной системы, наличием неразрешенного ПО**		
23.2.	Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности**		
23.3.	Угроза установки ПО/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		
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 ПО, сетевое ПО
24.3.	Угроза перехвата данных**		
24.4.	Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена		

1	2	3	4
24.5.	Угроза перехвата данных с сетевых портов		
24.6.	Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа**		

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

Список использованных сокращений:
ВЧ – высокочастотный;
ЕСЭДД – единая система электронного документооборота и делопроизводства;
ИСПДн – информационная система персональных данных;
ПО – программное обеспечение;
ПЭВМ – персональная электронно-вычислительная машина (АРМ);
реестр – стандартный реестр операционной системы;
ТС – технические средства.

Приложение № 2
к Положению об определении
актуальных угроз безопасности
персональных данных при их
обработке в информационных
системах персональных данных
Республики Татарстан

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 в пределах контролируемой зоны		
2.	Проведение атак на этапе эксплуатации средств криптографической защиты информации на следующие объекты: документация на средства криптографической защиты информации и компоненты среды функционирования средств криптографической защиты информации; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (средств вычислительной техники), на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		

1	2	3	4
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведения о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведения о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		
4.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий		
5.	Физический доступ к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среды функционирования средств криптографической защиты информации		
6.	Возможность воздействовать на аппаратные компоненты средств криптографической защиты информации и среды функционирования средств криптографической защиты информации, ограниченная мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, и направленными на предотвращение и пресечение несанкционированных действий		
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование средств криптографической защиты информации и сред функционирования средств криптографической защиты информации, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения		

1	2	3	4
8.	Проведение лабораторных исследований средств криптографической защиты информации, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется средство криптографической защиты информации, 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 средств криптографической защиты информации и сред функционирования средств криптографической защиты информации, в том числе с использованием исходных текстов, входящих в среду функционирования средств криптографической защиты информации прикладного программного обеспечения, непосредственно использующего вызовы программных функций средств криптографической защиты информации		
10.	Создание способов, подготовка и проведение с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения		
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования средств криптографической защиты информации		
12.	Возможность воздействовать на любые компоненты средств криптографической защиты информации и сред функционирования средств криптографической защиты информации		

Примечание. Незаполненные ячейки вышеуказанной таблицы определяются в частных моделях угроз и нарушителя безопасности информации для каждой информационной системы персональных данных.