|  |  |  |
| --- | --- | --- |
| БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ  ШАРАН РАЙОНЫ  МУНИЦИПАЛЬ РАЙОНЫНЫҢ  БАЗГЫЯ АУЫЛ СОВЕТЫ  АУЫЛ БИЛӘМӘҺЕ ХӘКИМИӘТЕ  452632, Базгыя аулы, Үҙәк урам, 50 тел.(34769) 2-42-35, e-mail:basgss@yandex.ru |  | РЕСПУБЛИКА БАШКОРТОСТАН  АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ  БАЗГИЕВСКИЙ СЕЛЬСОВЕТ  МУНИЦИПАЛЬНОГО РАЙОНА  ШАРАНСКИЙ РАЙОН  452632, c. Базгиево, ул.Центральная, 50  тел.(34769) 2-42-35, e-mail:basgss@yandex.ru |

**ҠАРАР ПОСТАНОВЛЕНИЕ**

«03» октябрь 2022 й. №38 «03» октября 2022 г.

**Об утверждении Положения об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан**

В соответствии с Указом Главы Республики Башкортостан от 18 февраля 2019 года № УГ-40 «Об утверждении Положения об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах государственных органов Республики Башкортостан и (или) подведомственных им организаций»,

ПОСТАНОВЛЯЮ:

1. Утвердить прилагаемое [Положение](consultantplus://offline/ref=E655A0FAA4C9F4176666060B124286689F671D060ED6712F1116018D54D5C89DF18B8074B512D7C804D0B106EED11F6AD220737541BFEFA3BF876B9DY570J) об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан.
2. Контроль исполнения настоящего постановления оставляю за собой.

Глава сельского поселения Т.А.Закиров

|  |
| --- |
| Приложение  к постановлению администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан  от «03» октября 2022 года №38 |

[Положение](consultantplus://offline/ref=E655A0FAA4C9F4176666060B124286689F671D060ED6712F1116018D54D5C89DF18B8074B512D7C804D0B106EED11F6AD220737541BFEFA3BF876B9DY570J)

об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящее Положение определяет перечень угроз безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан (далее - Администрация) при осуществлении ими соответствующих видов деятельности с учетом содержания, характера и способов обработки персональных данных.

В настоящем Положении используются следующие термины и их определения:

персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному либо определяемому физическому лицу (субъекту ПДн);

информационная система персональных данных (далее - ИСПДн) - совокупность информационных технологий и технических средств, содержащихся в базах данных и обеспечивающих обработку ПДн;

оператор ИСПДн - государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно либо совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием либо без использования средств автоматизации с ПДн, включая их сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение;

безопасность ПДн - состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн;

конфиденциальность ПДн - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн либо наличия иного законного основания;

несанкционированный доступ (далее - НСД) - доступ к информации или действия с ней, осуществляемые с нарушением установленных прав и (или) правил доступа к информации либо действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

доступ к информации - возможность ее получения и использования;

пользователь ИСПДн - лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования;

правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к его объектам;

информационный ресурс - часть ИСПДн, хранящая ПДн в файлах (базах данных) и (или) обеспечивающая доступ пользователей к ИСПДн;

средства вычислительной техники (далее - СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

средства криптографической защиты информации (далее - СКЗИ) - совокупность программных и технических средств, реализующих криптографические преобразования с исходной информацией и функции выработки и проверки электронной подписи;

среда функционирования СКЗИ (далее - СФ) - СКЗИ и компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ;

угрозы безопасности персональных данных (далее - УБПДн) - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатами которого могут стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при обработке ПДн в ИСПДн;

нарушитель безопасности ПДн - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн;

целостность информации - способность СВТ или информационной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного ее искажения (разрушения);

доступность информации - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

государственная доверенная инфокоммуникационная инфраструктура Республики Башкортостан (далее - ГДИИ РБ) - единая инфраструктура, реализующая пространство электронного взаимодействия и обеспечивающая предоставление инфокоммуникационных услуг (сервисов) на основе доверенных сетей связи;

оператор ГДИИ РБ - организация, в ведении которой находится ГДИИ РБ и которая обеспечивает сопровождение, администрирование и модернизацию ГДИИ РБ, а также защиту обрабатываемой в ней информации;

координатор ГДИИ РБ - Министерство цифрового развития государственного управления Республики Башкортостан, регулирующий вопросы подключения к ГДИИ РБ, государственный заказчик работ, связанных с развитием и сопровождением ГДИИ РБ;

республиканский центр обработки данных (далее - РЦОД) - основной сегмент инфраструктуры хранения и обработки данных, обеспечивающий защищенное хранение и обработку информации, содержащейся в информационных системах органов государственной власти Республики Башкортостан и в иных информационных системах;

системное программное обеспечение (далее - СПО) - совокупность программ для управления аппаратурой компьютера и обеспечения работы прикладных программ;

прикладное программное обеспечение (далее - ППО) - совокупность программ для решения прикладных задач (задач пользователя);

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

идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

вредоносное программное обеспечение - программа, предназначенная для осуществления НСД и (или) воздействия на ПДн либо ресурсы ИСПДн;

недекларированные возможности - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и (или) целостности обрабатываемой информации;

уровень защищенности ПДн - комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности ИСПДн.

Настоящее Положение разработано в соответствии со следующими нормативными актами и руководящими документами:

Федеральным [законом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D832F1EB97B7174D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) «Об информации, информационных технологиях и о защите информации»;

Федеральным [законом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D832F1EB95B6124D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) «О персональных данных»;

[Постановлением](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D837F0EE94B7154D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[Приказом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D835F6EC9FBB104D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) Федеральной службы по техническому и экспертному контролю (далее - ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[Приказом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D835F6EF9FB71A4D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[методикой](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D831F4E196B618102D6F1360301172CBD8BBE48E9F5A9F54DBD3A0DA2D4DH0K) определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14 февраля 2008 года;

базовой [моделью](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D83FFAEF91B018102D6F1360301172CBD8BBE48E9F5A9F54DBD3A0DA2D4DH0K) угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 15 февраля 2008 года;

методическим [документом](consultantplus://offline/ref=90E83EADED0DA4790997C7449456C2D837F6E09EB5164D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) «Меры защиты информации в государственных информационных системах№, утвержденным ФСТЭК России 11 февраля 2014 года;

[Приказом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D837F5EE9FB4114D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Указом Главы Республики Башкортостан от 18 февраля 2019 года № УГ-40 «Об утверждении Положения об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах государственных органов Республики Башкортостан и (или) подведомственных им организаций»;

[Постановлением](consultantplus://offline/ref=90E83EADED0DA4790997D949823A9DD136F8B79AB3174E773E1D6A65492D9288FCB588CB0FC500D6CDA6C42ED2921CD9F246H0K) Правительства Республики Башкортостан от 25 сентября 2015 года № 408 «О Концепции государственной доверенной инфокоммуникационной инфраструктуры Республики Башкортостан».

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

Настоящее Положение предназначено для Администрации при решении следующих задач:

определение УБПДн, актуальных при обработке ПДн в ИСПДн;

анализ защищенности ИСПДн от актуальных УБПДн в ходе выполнения мероприятий по обеспечению информационной безопасности (защите информации);

модернизация системы защиты ПДн;

проведение мероприятий по минимизации и (или) нейтрализации УБПДн;

предотвращение несанкционированного воздействия на компоненты ИСПДн;

контроль обеспечения требуемого уровня защищенности ПДн.

При определении УБПДн, актуальных при обработке ПДн в используемых ИСПДн, и совокупности предположений о возможностях нарушителя, которые могут использоваться при создании, подготовке и проведении компьютерных атак, Администрация с учетом вида, условий и особенностей функционирования ИСПДн, характера и способов обработки ПДн используют информацию:

о группах актуальных УБПДн, приведенных в [пункте 4.2.1](#Par266) настоящего Положения;

о типовых [возможностях](#Par328) нарушителей безопасности информации и направлениях компьютерных атак, приведенных в приложении № 1 к настоящему Положению;

о расширенном [перечне](#Par427) УБПДн, приведенном в приложении № 2 к настоящему Положению.

Определение актуальных УБПДн осуществляется в соответствии с нормативными актами уполномоченных федеральных органов исполнительной власти, а также настоящим Положением.

Определение требований к системе защиты информации в ИСПДн в зависимости от уровня их защищенности и УБПДн, принятых актуальными при обработке ПДн в ИСПДн, а также осуществление выбора средств защиты информации проводятся согласно нормативным правовым актам ФСБ России и ФСТЭК России, изданным во исполнение [части 4 статьи 19](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D832F1EB95B6124D27674A6C32167D94DDBCF58E9E5E8156D3C9A98E7E96D913D9F47C15A7CB98FD3746H0K) Федерального закона «О персональных данных».

Определение актуальных УБПДн применительно к ИСПДн Администрации осуществляется на основе расширенного [перечня](#Par427) УБПДн, прилагаемого к настоящему Положению, в рамках разработки частной модели УБПДн для конкретной ИСПДн.

В частной модели УБПДн приводятся описание ИСПДн и ее структурно-функциональных характеристик, а также описание УБПДн, в том числе возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов и последствий реализации УБПДн.

Типовая форма частной модели угроз безопасности информации для государственных органов разрабатывается координатором ГДИИ РБ с учетом требований [Приказа](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D835F6EC9FBB104D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», [Приказа](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D837F5EE9FB4114D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и банка данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/threat).

**2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Администрация обрабатывает ПДн в целях осуществления своих полномочий. Состав ПДн, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции), совершаемые с ПДн в ИСПДн, определяются Администрацией, являющейся оператором ИСПДн.

Порядок обработки ПДн в ИСПДн определяется требованиями Федерального [закона](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D832F1EB95B6124D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) «О персональных данных». Содержание и объем обрабатываемых ПДн в ИСПДн должны соответствовать целям их обработки.

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

В зависимости от технологии обработки ПДн, их целей и состава ИСПДн подразделяются на следующие категории:

информационно-справочные;

региональные;

ведомственные;

служебные.

Для всех категорий ПДн вышеуказанных видов ИСПДн необходимо обеспечивать следующие характеристики безопасности:

конфиденциальность;

целостность;

доступность.

**2.1. Размещение информационных систем персональных данных**

2.1.1. Серверы и базы данных ИСПДн Администрации могут располагаться непосредственно в Администрации или в РЦОД. Информационные ресурсы ИСПДн, которые относятся к государственным информационным системам, в обязательном порядке размещаются в РЦОД. При этом в Администрации функционируют СВТ, входящие в состав автоматизированных рабочих мест пользователей ИСПДн.

2.1.2. Контролируемой зоной ИСПДн, функционирующих в Администрации, являются здания и отдельные помещения, принадлежащие Администрации или арендуемые ею. СВТ, предназначенные для обработки ПДн, должны располагаться в пределах контролируемой зоны Администрации и РЦОД (для ИСПДн, по которым есть решение координатора ГДИИ РБ по размещению серверной части в РЦОД). 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 Администрации.

2.1.3. Локальные вычислительные сети передачи данных в Администрации организованы по топологии "звезда" и имеют подключения к следующим сетям:

внешним сетям общего пользования (сетям провайдера) посредством проводных каналов связи (оптоволокно или медные линии);

ГДИИ РБ посредством защищенных каналов связи, подключение к которым осуществляется в пределах контролируемой зоны;

иным сетям, взаимодействие с которыми организовано Администрацией в целях осуществления своих полномочий.

2.1.4. Подключение к сетям связи общего пользования осуществляется Администрацией при условии соблюдения ими мер по обеспечению безопасности информации.

2.1.5. Защищенное подключение к ГДИИ РБ осуществляет оператор ГДИИ РБ в соответствии со своими регламентами.

**2.2. Объекты защиты и технологии обработки персональных**

**данных в информационных системах персональных данных**

2.2.1. При определении Администрацией УБПДн в конкретной ИСПДн защите подлежат следующие входящие в нее объекты:

ПДн, обрабатываемые в ИСПДн;

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

СВТ, предназначенные для обработки ПДн;

средства защиты информации и СКЗИ;

среда функционирования СКЗИ;

информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ, а также на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в ИСПДн, в том числе в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

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

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

помещения, в которых обрабатываются ПДн и располагаются компоненты ИСПДн;

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

2.2.2. В состав СВТ, предназначенных для обработки ПДн в ИСПДн, входят:

автоматизированное рабочее место (далее - АРМ) с различными уровнями доступа (правами), представляющее собой программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к ИСПДн и предназначенный для локальной обработки информации (ИСПДн может состоять из одного АРМ);

терминальная станция, представляющая собой программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к ИСПДн и не предназначенный для локальной обработки информации;

серверный сегмент ИСПДн, предназначенный для обработки и консолидированного хранения ПДн и представляющий собой программно-аппаратный комплекс в совокупности с программным и информационным обеспечением для его управления:

СПО (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.);

ППО (системы управления базами данных и т.п.), предназначенное для обработки и консолидированного хранения данных в ИСПДн.

**3. ВИДЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**3.1. Информационно-справочные информационные системы**

**персональных данных**

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

3.1.1. К информационно-справочным ИСПДн относятся:

официальные порталы (сайты) Администрации;

информационные порталы (сайты), которые ведутся Администрацией и посвящаются определенному проекту и (или) мероприятию, проводимому на территории Республики Башкортостан;

закрытые порталы для нескольких групп сотрудников Администрации.

3.1.2. Официальные порталы (сайты) Администрации содержат сведения об их деятельности, в том числе сведения, подлежащие обязательному опубликованию в данных ИСПДн в соответствии с законодательством Российской Федерации.

Категории ПДн, которые могут подлежать обработке в ИСПДн, - иные и (или) общедоступные.

Режим обработки ПДн в информационно-справочных ИСПДн - многопользовательский, предусматривающий разграничение доступа. Обработка ПДн осуществляется посредством веб-интерфейса сотрудниками оператора ИСПДн или сторонней организации по поручению оператора ИСПДн. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами доступа.

Обработке в ИСПДн могут подлежать ПДн сотрудников оператора ИСПДн или субъектов ПДн, не являющихся сотрудниками оператора ИСПДн.

Структура ИСПДн - локальная, функционирующая в контролируемой зоне Администрации, и (или) на серверном оборудовании Администрации в пределах контролируемой зоны, и (или) на вычислительных ресурсах РЦОД.

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

подключенные посредством ГДИИ РБ;

подключенные с использованием иных каналов связи.

Технические средства (далее - ТС), предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

**3.2. Региональные информационные системы персональных данных**

Региональные ИСПДн эксплуатируются по решению Администрации.

3.2.1. По выполняемым функциям ИСПДн подразделяются на следующие:

интеграционные (система межведомственного электронного взаимодействия Республики Башкортостан; узел обмена системы электронного документооборота органов и т.п.);

многопрофильные (например, автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг Республики Башкортостан; региональная информационная система в сфере закупок и т.п.).

3.2.2. Интеграционные ИСПДн содержат сведения о мероприятиях, проводимых Администрацией в соответствии с их функциями и полномочиями.

Категории ПДн, которые могут подлежать обработке в данных ИСПДн: иные; общедоступные.

Режим обработки ПДн в интеграционных ИСПДн - многопользовательский, предусматривающий разграничение прав доступа. Обработка ПДн осуществляется посредством веб-интерфейса сотрудниками оператора ИСПДн или сторонней организацией по поручению оператора ИСПДн. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами доступа.

Структура ИСПДн - локальная или распределенная, функционирующая в контролируемой зоне Администрации.

ИСПДн могут быть подключены к сетям связи общего пользования (сетям международного информационного обмена). По типу подключения интеграционные ИСПДн делятся на: подключенные посредством ГДИИ РБ; подключенные с использованием иных каналов связи.

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

посредством ГДИИ РБ;

с использованием иных средств защищенного доступа для передачи информации по открытым каналам связи.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ; серверное, сетевое и телекоммуникационное оборудование.

3.2.3. Многопрофильные ИСПДн консолидируют сведения из множества органов местного самоуправления муниципального района Шаранский район Республики Башкортостан, касающиеся их финансовой и другой деятельности в соответствии с функциями и полномочиями.

Категории ПДн, которые могут подлежать обработке в данной ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки ПДн в многопрофильных ИСПДн - многопользовательский, предусматривающий разграничение прав доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами доступа.

Структура ИСПДн - локальная или распределенная, функционирующая в контролируемой зоне Администрации и (или) РЦОД.

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

подключенные посредством ГДИИ РБ;

подключенные с использованием иных каналов связи.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

**3.3. Ведомственные информационные системы персональных данных**

Ведомственные ИСПДн создаются (эксплуатируются) по решению Администрации для осуществления своих функций.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки ПДн в ведомственных ИСПДн - многопользовательский, предусматривающий разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники оператора ИСПДн и субъекты персональных данных, не являющиеся сотрудниками оператора.

Структура ИСПДн - распределенная или локальная, функционирующая в контролируемой зоне Администрации и (или) РЦОД (в случае принятия такого решения координатором ГДИИ РБ).

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

подключенные посредством ГДИИ РБ;

подключенные с использованием иных каналов связи.

Обмен ПДн между сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется: посредством ГДИИ РБ; с использованием СКЗИ через сети общего пользования.

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

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; терминальная станция; серверное, сетевое и телекоммуникационное оборудование.

**3.4. Служебные информационные системы персональных данных**

Служебные ИСПДн создаются (эксплуатируются) по Администрации в их интересах; цели и задачи создания (модернизации), эксплуатации служебных ИСПДн определяются Администрацией и используются для автоматизации определенной области деятельности или типовой деятельности, неспецифичной относительно полномочий Администрации.

3.4.1. К основным служебным ИСПДн относятся:

ИСПДн бухгалтерского учета и управления финансами;

ИСПДн кадрового учета и управления персоналом;

ИСПДн документооборота и делопроизводства.

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

Обработке в ИСПДн подлежат иные категории ПДн.

Режим обработки ПДн в служебных ИСПДн - многопользовательский, предусматривающий разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами доступа.

Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники оператора ИСПДн или сторонней организации по поручению оператора ИСПДн.

Структура ИСПДн - локальная, функционирующая в контролируемой зоне Администрации.

По типу подключения ИСПДн делятся на:

ИСПДн без подключения к сетям связи общего пользования (передача ПДн осуществляется с использованием машинных носителей);

подключенные посредством ГДИИ РБ;

подключенные с использованием иных каналов связи.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

3.4.3. ИСПДн кадрового учета и управления персоналом предназначены для автоматизации деятельности Администрации, связанной с ведением кадрового учета и управления персоналом.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

специальные;

иные.

Режим обработки ПДн в ИСПДн кадрового учета - многопользовательский, предусматривающий разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных и (или) стандартных офисных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами доступа.

Типы субъектов, ПДн которых могут подлежать обработке в данной ИСПДн: сотрудники оператора ИСПДн; граждане Российской Федерации, устанавливающие (имеющие) трудовые отношения с Администрацией.

Структура ИСПДн - локальная, функционирующая в контролируемой зоне Администрации.

По типу подключения ИСПДн делятся на:

ИСПДн без подключения к сетям связи общего пользования (передача ПДн осуществляется с использованием машинных носителей);

подключенные посредством ГДИИ РБ;

подключенные через провайдера.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

3.4.4. ИСПДн пенсионного фонда и налоговых служб предназначены для автоматизации деятельности Администрации, связанной с осуществлением пенсионных отчислений и уплатой налогов.

Режим обработки ПДн в ИСПДн пенсионного фонда - многопользовательский, предусматривающий разграничение прав доступа.

Обработка ПДн осуществляется сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами доступа.

Тип субъектов, ПДн которых могут подлежать обработке в данной ИСПДн, - сотрудники оператора ИСПДн.

Структура ИСПДн - локальная, функционирующая в контролируемой зоне Администрации.

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

подключенные посредством ГДИИ РБ;

подключенные с использованием иных каналов связи.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

3.4.5. ИСПДн документооборота и делопроизводства предназначены для автоматизации деятельности Администрации, связанной с осуществлением документооборота и делопроизводства.

Категории ПДн, которые могут подлежать обработке в данной ИСПДн:

общедоступные;

специальные;

иные.

Режим обработки ПДн в указанной ИСПДн - многопользовательский, предусматривающий разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

Типы субъектов, ПДн которых могут подлежать обработке в указанной ИСПДн: сотрудники оператора ИСПДн и (или) субъекты персональных данных, не являющиеся сотрудниками оператора.

Структура ИСПДн - локальная, функционирующая в контролируемой зоне Администрации.

По типу подключения ИСПДн делятся на:

ИСПДн без подключения к сетям связи общего пользования (передача ПДн осуществляется с использованием машинных носителей);

подключенные с использованием иных каналов связи.

ТС, предназначенные для обработки ПДн: СВТ, входящие в состав АРМ пользователей ИСПДн; серверное, сетевое и телекоммуникационное оборудование.

**4. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ**

**4.1. Источники угроз безопасности персональных данных**

4.1.1. Источниками УБПДн в ИСПДн выступают:

носитель вредоносной программы;

аппаратная закладка;

нарушитель.

4.1.2. 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 носителей рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD, DVD и др.), флэш-память, отчуждаемый жесткий диск и др.;

встроенные носители информации (жесткие диски, микросхемы оперативной памяти, 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 др.).

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 др.).

4.1.3. Аппаратная закладка предназначена для регистрации информации (ПДн), вводимой в ИСПДн с клавиатуры АРМ пользователя ИСПДн:

аппаратная закладка внутри клавиатуры;

считывание данных с кабеля клавиатуры бесконтактным методом;

включение устройства в разрыв кабеля;

аппаратная закладка внутри системного блока и др.

При условии исключения неконтролируемого пребывания физических лиц в служебных помещениях, в которых размещены носители ПДн, компоненты ИСПДн, угроза установки аппаратных закладок посторонними лицами рассматривается как неактуальная. Также вероятность реализации данной угрозы считается низкой из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и ценности, полученной в результате информации.

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

По наличию права постоянного или разового доступа к ИСПДн нарушители подразделяются на три типа.

Первый тип - внешний нарушитель. Данный тип нарушителя не имеет права постоянного доступа или имеет право разового доступа в контролируемую зону, а также не имеет доступа к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны, либо действия нарушителя ограничены и контролируются. Данный тип нарушителя может реализовывать угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Второй тип - внутренний нарушитель, имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа в контролируемую зону, а также доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Данный тип нарушителя может осуществлять компьютерные атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн.

Третий тип - внутренний нарушитель, не имеющий доступа к ИСПДн. Данный тип нарушителя имеет право постоянного (периодического) доступа в контролируемую зону, но не имеет доступа к техническим средствам и ресурсам ИСПДн, расположенным в пределах контролируемой зоны. Данный тип нарушителя может осуществлять компьютерные атаки с использованием внутренней (локальной) сети передачи данных.

**4.2. Основные группы угроз безопасности персональных данных**

**в информационных системах персональных данных**

4.2.1. Основными группами УБПДн в ИСПДн являются:

угрозы утечки информации по техническим каналам;

угрозы нарушения конфиденциальности;

угрозы нарушения доступности информации;

угрозы нарушения целостности информации;

угрозы, не относящиеся к компьютерным атакам;

угрозы использования штатных средств ИСПДн в целях совершения НСД к информации;

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

угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

угрозы внесения уязвимостей при проектировании и внедрении ИСПДн (системы защиты ИСПДн);

угрозы ошибочных (деструктивных) действий сотрудников оператора ИСПДн;

угрозы программно-математических воздействий;

угрозы, связанные с использованием сетевых технологий;

угрозы, связанные с использованием облачных технологий;

угрозы, связанные с использованием технологий виртуализации;

угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи;

угрозы, связанные с нарушением правил эксплуатации машинных носителей;

угрозы, связанные с нарушением процедур установки (обновления) программного обеспечения и оборудования;

угрозы физического доступа к компонентам ИСПДн;

угрозы недекларированных возможностей в СПО и ППО;

угрозы эксплуатации уязвимостей в СПО, ППО, в аппаратных компонентах ИСПДн, микропрограммном обеспечении, а также в средствах защиты информации;

угрозы инженерной инфраструктуры;

угрозы, связанные с отсутствием системы регистрации событий информационной безопасности.

**5. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Перечень актуальных УБПДн уточняется и дополняется по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн в ходе периодических мероприятий по оценке состояния ее защищенности.

Периодические мероприятия включают в себя анализ изменения и переоценку актуальных УБПДн. Периодические мероприятия проводятся не реже одного раза в год оператором ГДИИ РБ с привлечением экспертного сообщества.

Результаты переоценки угроз безопасности персональных данных согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

**6. МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Организационными мерами защиты ПДн при их обработке в ИСПДн являются:

разработка (актуализация) документов, регламентирующих вопросы обеспечения безопасности ПДн и эксплуатации средств защиты информации в ИСПДн;

определение технологических процессов обработки ПДн;

разработка (актуализация) инструкций по вопросам эксплуатации ИСПДн для пользователей, администраторов и администраторов безопасности;

охрана и организация режима допуска к компонентам ИСПДн;

размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

учет машинных носителей ПДн и средств защиты информации.

6.2. Техническими мерами защиты ПДн при их обработке в ИСПДн являются следующие:

использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности информации для защиты от несанкционированного доступа (класс средств защиты определяется в соответствии с [Приказом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D835F6EF9FB71A4D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

использование СКЗИ в случаях актуальных угроз, нейтрализация которых возможна только с помощью криптографической защиты (класс средств криптографической защиты определяется в соответствии с [Приказом](consultantplus://offline/ref=90E83EADED0DA4790997D95F8156C2D837F5EE9FB4114D27674A6C32167D94DDAEF5D6925E854BDACDBCD82FD048HEK) ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»);

использование средств антивирусной защиты с регулярным обновлением баз данных признаков вредоносных компьютерных программ (вирусов);

использование средств контроля (анализа) защищенности ИСПДн;

периодическое резервное копирование информации на резервные машинные носители информации.

6.3. Оценка эффективности мер по обеспечению безопасности ПДн, реализованных в рамках системы защиты ПДн, проводится оператором ИСПДн самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

6.4. В случае, если функции использования информационных технологий Администрация передала иным организациям, обеспечение мер защиты ПДн при их обработке в ИСПД возлагается на указанные организации в соответствии с заключенными соглашениями, договорами и законодательством Российской Федерации.

|  |
| --- |
| Приложение № 1  к [Положению](consultantplus://offline/ref=E655A0FAA4C9F4176666060B124286689F671D060ED6712F1116018D54D5C89DF18B8074B512D7C804D0B106EED11F6AD220737541BFEFA3BF876B9DY570J) об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан |

**ТИПОВЫЕ ВОЗМОЖНОСТИ**

**НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И НАПРАВЛЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы) | Актуальность использования угроз для построения и реализации атак | Обоснование отсутствия угрозы |
| 1 | 2 | 3 | 4 |
| 1 | Проведение атаки при нахождении за пределами контролируемой зоны |  |  |
| 2 | Проведение атаки при нахождении в пределах контролируемой зоны |  |  |
| 3 | Проведение атаки на этапе эксплуатации СКЗИ на следующие объекты:  документация на СКЗИ и компоненты СФ;  помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ |  |  |
| 4 | Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:  сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;  сведений о мерах по обеспечению безопасности информации контролируемой зоны объектов, в которых размещены ресурсы ИС;  сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ |  |  |
| 5 | Использование штатных средств ИС, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |  |  |
| 6 | Физический доступ к СВТ, на которых реализованы СКЗИ и СФ |  |  |
| 7 | Воздействие на аппаратные компоненты СКЗИ и СФ, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |  |  |
| 8 | Создание способов компьютерных атак, их подготовка и проведение с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО |  |  |
| 9 | Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий |  |  |
| 10 | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) возможностей системного ПО |  |  |
| 11 | Наличие сведений, содержащихся в конструкторской документации на аппаратные и программные компоненты СФ |  |  |
| 12 | Воздействие на любые компоненты СКЗИ и СФ |  |  |

**Список использованных сокращений**

|  |  |  |
| --- | --- | --- |
| ИС | - | информационная система |
| ПО | - | программное обеспечение |
| СВТ | - | средства вычислительной техники |
| СКЗИ | - | средства криптографической защиты информации |
| СФ | - | среда функционирования |

Примечание. Заполнение ячеек таблицы зависит от частных моделей угроз и нарушителя безопасности информации для каждой информационной системы персональных данных.

|  |
| --- |
| Приложение № 2  к [Положению](consultantplus://offline/ref=E655A0FAA4C9F4176666060B124286689F671D060ED6712F1116018D54D5C89DF18B8074B512D7C804D0B106EED11F6AD220737541BFEFA3BF876B9DY570J) об угрозах безопасности персональных данных, актуальных при их обработке в информационных системах администрации сельского поселения Базгиевский сельсовет муниципального района Шаранский район Республики Башкортостан |

**РАСШИРЕННЫЙ ПЕРЕЧЕНЬ**

**УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование угроз безопасности персональных данных в информационных системах персональных данных | Источники угроз безопасности персональных данных | Объект воздействия |
| 1 | 2 | 3 | 4 |
|  | 1. Угрозы утечки информации по техническим каналам | | |
|  | * 1. Угрозы утечки акустической информации | | |
| 1.1.1 | Использование направленных (ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.1.2 | Использование "контактных микрофонов" для съема виброакустических сигналов | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.1.3 | Использование "лазерных микрофонов" для съема виброакустических сигналов | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.1.4 | Использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет "микрофонного эффекта" в ТС обработки информации и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений) | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.1.5 | Применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки информации и ВТСС ВЧ-сигналом | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.1.6 | Применение акустооптических модуляторов на базе волоконно-оптической системы, находящихся в поле акустического сигнала ("оптических микрофонов") | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
|  | * 1. Угрозы утечки видовой информации | | |
| 1.2.1 | Визуальный просмотр на экранах дисплеев и других средств отображения СВТ и ИВК, входящих в состав ИС | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.2.2 | Визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ и ИВК, входящих в состав ИС | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.2.3 | Использование специальных электронных устройств съема видовой информации (видеозакладки) | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
|  | * 1. Угрозы утечки информации по каналам побочных электромагнитных излучений | | |
| 1.3.1 | Применение специальных средств регистрации ПЭМИН от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры) | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.3.2 | Применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых ТС, на цепи электропитания и линий связи, выходящих за пределы служебных помещений | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.3.3 | Применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИС или при наличии паразитной генерации в узлах ТС | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
| 1.3.4 | Применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИС, в которых проводится обработка информативных сигналов - параметрических каналов утечки | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с высоким потенциалом | файлы БД системы;  файлы сканов документов в виде электромагнитного излучения |
|  | 1. Угрозы использования штатных средств информационных систем с целью совершения несанкционированного доступа к информации | | |
| 2.1 | Угроза некорректного использования функционала программного обеспечения | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  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 | СПО;  ППО;  сетевое ПО;  микропрограммное обеспечение;  реестр |
| 2.3 | Угроза несанкционированного изменения аутентификационной информации | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  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 |
| 2.5 | Угроза доступа в операционную среду (локальную ОС отдельных ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | - | - |
|  | 1. Угрозы нарушения доступности информации | | |
| 3.1 | Угроза длительного удержания вычислительных ресурсов пользователями | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | ИС;  сетевой узел;  носитель информации;  СПО;  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 | ИС;  сетевой узел;  СПО;  сетевое ПО;  сетевой трафик |
| 3.9 | Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | ИС;  сетевой узел;  СПО;  сетевое ПО |
| 3.10 | Угроза утраты вычислительных ресурсов | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | ИС;  сетевой узел;  носитель информации;  СПО;  сетевое ПО;  сетевой трафик |
| 3.11 | Угроза вывода из строя (выхода из строя) отдельных ТС | - | - |
| 3.12 | Угроза вывода из строя незарезервированных ТС, 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 ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | - | - |
| 3.17 | Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена "неожидаемой" информации | - | - |
|  | 1. 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 | СПО;  ППО;  сетевое ПО |
| 4.4 | Угроза подмены содержимого сетевых ресурсов | внешний нарушитель с низким потенциалом | ППО;  сетевое ПО;  сетевой трафик |
| 4.5 | Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | внутренний нарушитель с низким потенциалом | ИС;  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;  СПО |
| 4.7 | Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | - | - |
| 4.8 | Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | - | - |
| 4.9 | Угроза отсутствия контроля за поступающими в ИС данными, в том числе незапрашиваемыми | - | - |
| 4.10 | Отсутствие средств централизованного управления за поступающими в ИС данными, в том числе незапрашиваемыми | - | - |
| 4.11 | Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | - | - |
| 4.12 | Угроза доступа в ИС информации от неаутентифицированных серверов (пользователей) | - | - |
| 4.13 | Угроза отсутствия контроля за данными, передаваемыми из ИС | - | - |
| 4.14 | Отсутствие резервного копирования информации, передаваемой из ИС | - | - |
| 4.15 | Угроза передачи из ИС недопустимой информации | - | - |
| 4.16 | Угроза отсутствия контроля за данными, вводимыми в систему пользователями | - | - |
| 4.17 | Угроза ввода (передачи) недостоверных (ошибочных) данных | - | - |
| 4.18 | Угроза подмены используемых ИС файлов | - | - |
| 4.19 | Угроза модификации (удаления) файлов журналов системного ПО, ППО, СЗИ | - | - |
| 4.20 | Угроза установки (запуска) модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | - | - |
| 4.21 | Угроза модификации (стирания, удаления) данных системы регистрации событий информационной безопасности | - | - |
| 4.22 | Отсутствие регламента (графика) проведения контроля целостности применяемых программных средств, в том числе СЗИ | - | - |
| 4.23 | Угроза отсутствия контроля целостности информации, обрабатываемой ИС, и ее структуры | - | - |
|  | 5.Угрозы недекларируемых возможностей в системном и прикладном программном обеспечении | | |
| 5.1 | Угроза перебора всех настроек и параметров приложения | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО;  микропрограммное обеспечение;  реестр |
| 5.2 | Угроза возникновения ошибок функционирования СПО, реализация недекларированных возможностей системного ПО | - | - |
| 5.3 | Угроза использования встроенных недекларированных возможностей для получения несанкционированного доступа к ИС | - | - |
|  | 6. Угрозы, не являющиеся атаками | | |
| 6.1 | Угроза исчерпания вычислительных ресурсов хранилища больших данных | внутренний нарушитель с низким потенциалом | ИС |
| 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 персональной электронно-вычислительной машине при выводе из промежуточных состояний питания | внутренний нарушитель с низким потенциалом | рабочая станция;  носитель информации;  СПО;  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 ТС, программных средств, каналов связи |  |  |
|  | 1. Угрозы 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 |
| 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 | СПО;  сетевое ПО |
| 7.4 | Угроза программного сброса пароля BIOS | внутренний нарушитель с низким потенциалом | микропрограммное обеспечение BIOS/UEFI;  СПО |
| 7.5 | Угроза "кражи" учетной записи доступа к сетевым сервисам | внешний нарушитель с низким потенциалом | сетевое ПО |
| 7.6 | Угроза получения доступа к ИС, ее компонентам, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | - | - |
| 7.7 | Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | - | - |
| 7.8 | Угроза получения несанкционированного доступа в результате сбоев (ошибок) подсистемы идентификации и аутентификации | - | - |
| 7.9 | Угроза получения несанкционированного доступа сторонними лицами, устройствами | - | - |
| 7.10 | Угроза отсутствия (слабости) процедур аутентификации при доступе пользователей (устройств) к ресурсам ИС | - | - |
| 7.11 | Угрозы авторизации с использованием устаревших, но не отключенных учетных записей | - | - |
| 7.12 | Угроза использования "слабых" методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | - | - |
| 7.13 | Угроза применения только программных методов двухфакторной аутентификации | - | - |
| 7.14 | Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | - | - |
| 7.15 | Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | - | - |
| 7.16 | Угроза доступа к ИС неаутентифицированных устройств и пользователей | - | - |
| 7.17 | Угроза повторного использования идентификаторов в течение как минимум 1 года | - | - |
| 7.18 | Угроза использования идентификаторов, не используемых более 45 дней | - | - |
| 7.19 | Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | - | - |
| 7.20 | Отсутствие управления идентификаторами внешних пользователей | - | - |
| 7.21 | Угроза использования "слабых" (предсказуемых) паролей | - | - |
| 7.22 | Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | - | - |
| 7.23 | Угроза использования пользователями идентичных идентификаторов в разных информационных системах | - | - |
| 7.24 | Угроза использования неподписанных программных средств | - | - |
| 7.25 | Угроза запуска несанкционированных процессов и служб от имени системных пользователей | - | - |
| 7.26 | Угроза отсутствия регламента работы с персональными идентификаторами | - | - |
| 7.27 | Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | - | - |
| 7.28 | Угроза бесконтрольного доступа пользователей к процессу загрузки | - | - |
| 7.29 | Угроза подмены (модификации) базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | - | - |
|  | 1. 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 | ИС;  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 ОС | 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 | СПО;  ППО;  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;  ППО;  СПО |
| 8.8 | Угроза использования информации идентификации (аутентификации), заданной по умолчанию | внешний нарушитель со средним потенциалом;  внутренний нарушитель с низким потенциалом | СЗИ;  СПО;  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 | СПО;  ППО;  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 | СПО;  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 |
| 8.17 | Угроза несанкционированного редактирования реестра | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО, использующее реестр;  реестр |
| 8.18 | Угроза несанкционированного создания учетной записи пользователя | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО |
| 8.19 | Угроза несанкционированного управления буфером | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  ППО;  сетевое ПО |
| 8.20 | Угроза несанкционированного управления синхронизацией и состоянием систем | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО;  микропрограммное обеспечение |
| 8.21 | Угроза несанкционированного управления указателями | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО |
| 8.22 | Угроза передачи запрещенных команд на оборудование с числовым программным управлением | внутренний нарушитель с низким потенциалом | СПО;  ППО |
| 8.23 | Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  аппаратное обеспечение |
| 8.24 | Угроза перехвата привилегированного потока | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО |
| 8.25 | Угроза перехвата привилегированного процесса | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО |
| 8.26 | Угроза повышения привилегий | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  сетевое ПО;  ИС |
| 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 | СПО |
| 8.29 | Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | - | ИС;  система разграничения доступа хранилища больших данных |
| 8.30 | Угроза удаления аутентификационной информации | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  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 | СПО;  ППО |
| 8.33 | Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | - | - |
| 8.34 | Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами (учетными записями), в том числе с повышенными правами доступа | - | - |
| 8.35 | Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | - | - |
| 8.36 | Угроза бесконтрольной передачи данных как внутри ИС, так и между такими системами | - | - |
| 8.37 | Угроза получения дополнительных данных, не предусмотренных технологией их обработки | - | - |
| 8.38 | Угроза получения разными пользователями, лицами, обеспечивающими функционирование систем, доступа к данным и полномочиям, не предназначенным для этих лиц в связи с их должностными обязанностями | - | - |
| 8.39 | Угроза предоставления пользователю прав доступа, не являющихся необходимыми для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | - | - |
| 8.40 | Угроза отсутствия ограничения на количество неудачных попыток входа в ИС | - | - |
| 8.41 | Угроза использования (подключения) к открытому (незаблокированному) сеансу пользователя | - | - |
| 8.42 | Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | - | - |
| 8.43 | Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | - | - |
| 8.44 | Угроза подбора идентификационных данных для удаленного доступа к ИС | - | - |
| 8.45 | Угроза использования слабостей (уязвимостей) защиты протоколов удаленного доступа | - | - |
| 8.46 | Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | - | - |
| 8.47 | Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе с мобильных устройств, без прохождения процедуры идентификации и авторизации | - | - |
| 8.48 | Угроза получения доступа к ИС с использованием технологий беспроводного доступа с неконтролируемых устройств | - | - |
| 8.49 | Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | - | - |
| 8.50 | Угроза получения несанкционированного доступа к средствам управления персональными идентификаторами (учетными записями), в том числе с повышенными правами доступа | - | - |
| 8.51 | Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | - | - |
| 8.52 | Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | - | - |
| 8.53 | Угроза бесконтрольного доступа к информации неопределенным кругом лиц | - | - |
| 8.54 | Угроза получения доступа к данным, не предназначенным для пользователя | - | - |
| 8.55 | Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | - | - |
| 8.56 | Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами | - | - |
| 8.57 | Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ней мобильных устройств | - | - |
| 8.58 | Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | - | - |
| 8.59 | Отсутствие отказоустойчивых централизованных средств управления учетными записями | - | - |
| 8.60 | Отсутствие автоматического блокирования учетных записей по истечении их срока действия в результате исчерпания попыток доступа к ИС, выявления попыток НСД | - | - |
| 8.61 | Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | - | - |
| 8.62 | Угроза передачи информации разной степени конфиденциальности без разграничения информационных потоков | - | - |
| 8.63 | Угроза передачи информации без соблюдения атрибутов (меток) безопасности, связанных с передаваемой информацией | - | - |
| 8.64 | Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений технологий обработки, передаваемых данных | - | - |
| 8.65 | Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | - | - |
| 8.66 | Угроза несанкционированного доступа к средствам управления информационными потоками | - | - |
| 8.67 | Угроза возложения функционально различных должностных обязанностей (ролей) на одно должностное лицо | - | - |
| 8.68 | Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | - | - |
| 8.69 | Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС и о количестве успешных (неуспешных) попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | - | - |
| 8.70 | Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | - | - |
| 8.71 | Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с двух и более) различных устройств | - | - |
| 8.72 | Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия 5 минут | - | - |
| 8.73 | Угроза использования незавершенных сеансов пользователей | - | - |
| 8.74 | Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты информации, в том числе с использованием технологий беспроводного доступа | - | - |
| 8.75 | Отсутствие автоматизированного мониторинга и контроля удаленного доступа | - | - |
| 8.76 | Угроза использования уязвимых (незащищенных) технологий удаленного доступа | - | - |
| 8.77 | Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | - | - |
| 8.78 | Отсутствие механизмов автоматизированного контроля параметров настройки компонентов ПО, влияющих на безопасность информации | - | - |
| 8.79 | Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов ПО, влияющих на безопасность информации | - | - |
| 8.80 | Отсутствие контроля за используемыми интерфейсами ввода (вывода) | - | - |
|  | 1. Угрозы ошибок (внесения уязвимостей) при проектировании и внедрении ИС (системы защиты ИС) | | |
| 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;  ТС;  ИС;  ключевая система информационной инфраструктуры |
| 9.3 | Угроза внедрения системной избыточности | внутренний нарушитель со средним потенциалом | ПО;  ИС;  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 | - | - |
|  | 1. Угрозы ошибочных (деструктивных) действий лиц | | |
| 10.1 | Угроза подмены действия пользователя путем обмана | внешний нарушитель со средним потенциалом | ППО;  сетевое ПО |
| 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 ИС, СЗИ и СКЗИ в соответствии установленными для них административными полномочиями | - | - |
| 10.4 | Угроза внесения изменений в конфигурацию программных средств и ТС, приводящих к отключению (частичному отключению) ИС (модулей, компонентов), СЗИ (в случае сговора с внешними нарушителями безопасности информации) | - | - |
| 10.5 | Угроза создания неконтролируемых точек доступа (лазеек) в систему для удаленного доступа к ИС | - | - |
| 10.6 | Угроза переконфигурирования СЗИ и СКЗИ для реализации угроз ИС | - | - |
| 10.7 | Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | - | - |
| 10.8 | Угроза хищения ключей шифрования, идентификаторов и известных паролей | - | - |
| 10.9 | Угроза внесения в программно-аппаратные средства ИС закладок, обеспечивающих съем информации, используя непосредственное подключение к ТС обработки информации | - | - |
| 10.10 | Создание методов и средств реализации атак на ИС, а также самостоятельное проведение атак | - | - |
| 10.11 | Ошибки при конфигурировании и обслуживании модулей (компонентов) ИС | - | - |
| 10.12 | Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и (или) модификация программного обеспечения; создание множественных ложных информационных сообщений) | - | - |
| 10.13 | Угроза несанкционированного съема информации, блокирования работы отдельных пользователей, перестройка планов маршрутизации и политики доступа сети | - | - |
| 10.14 | Угроза непреднамеренного разглашения ПДн лицам, не имеющим к ним прав доступа | - | - |
| 10.15 | Угроза нарушения правил хранения ключевой информации | - | - |
| 10.16 | Угроза передачи защищаемой информации по открытым каналам связи | - | - |
| 10.17 | Угроза несанкционированной модификации (уничтожения) информации легитимным пользователем | - | - |
| 10.18 | Угроза копирования информации на незарегистрированный носитель информации | - | - |
| 10.19 | Угроза несанкционированного отключения СЗИ | - | - |
| 10.20 | Угрозы вербовки пользователей (социальной инженерии) | - | - |
|  | 11. Угрозы нарушения конфиденциальности | | |
| 11.1 | Угроза исследования механизмов работы программы | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО;  микропрограммное обеспечение |
| 11.2 | Угроза исследования приложения через отчеты об ошибках | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  сетевое ПО;  микропрограммное обеспечение |
| 11.3 | Угроза обнаружения открытых портов и идентификации привязанных к нему 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;  ППО |
| 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 ИС, выявления протоколов, портов | - | - |
| 11.11 | Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе идентификаторов и паролей), их подмены | - | - |
| 11.12 | Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | - | - |
| 11.13 | Угроза получения нарушителем сведений о структуре, конфигурации, настройках и системы защиты ИС | - | - |
| 11.14 | Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | - | - |
| 11.15 | Угроза получения нарушителем идентификационных данных легальных пользователей ИС | - | - |
| 11.16 | Угроза разглашения пользователем сведений конфиденциального характера | - | - |
|  | 12. Угрозы программно-математических воздействий на ИС | | |
| 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 в ИС вредоносного кода или некорректных входных данных | внешний нарушитель с низким потенциалом | СПО;  ППО;  сетевое ПО |
| 12.3 | Угроза восстановления аутентификационной информации | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  микропрограммное обеспечение;  учетные данные пользователя |
| 12.4 | Угроза деструктивного изменения конфигурации (среды окружения) программ | внутренний нарушитель с низким потенциалом | СПО;  ППО;  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;  СПО;  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 информации, вводимой и выводимой на периферийные устройства | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  ППО;  сетевое ПО;  аппаратное обеспечение |
| 12.8 | Угроза использования слабостей кодирования входных данных | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  ППО;  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 |
| 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 | СПО;  ППО;  аппаратное обеспечение |
| 12.13 | Угроза подмены резервной копии программного обеспечения BIOS | внутренний нарушитель с низким потенциалом | микропрограммное и аппаратное обеспечение;  BIOS/UEFI |
| 12.14 | Угроза пропуска проверки целостности программного обеспечения | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  ППО;  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 | - | - |
| 12.20 | Угроза внедрения в ИС вредоносного ПО с устройств, подключаемых с использованием технологий беспроводного доступа | - | - |
| 12.21 | Применение специально созданных программных продуктов для НСД | - | - |
| 12.22 | Угроза внедрения вредоносного ПО через легитимные схемы информационного обмена между ИС | - | - |
| 12.23 | Отсутствие централизованной системы управления средствами антивирусной защиты | - | - |
|  | 13. Угрозы, связанные с использованием облачных услуг | | |
| 13.1 | Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг | внутренний нарушитель с низким потенциалом | облачная система;  виртуальная машина |
| 13.2 | Угроза злоупотребления доверием потребителей облачных услуг | внешний нарушитель с низким потенциалом | облачная система |
| 13.3 | Угроза конфликта юрисдикции различных стран | внешний нарушитель с низким потенциалом | облачная система |
| 13.4 | Угроза нарушения доступности облачного сервера | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | облачная система;  облачный сервер |
| 13.5 | Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения | внешний нарушитель с низким потенциалом | облачная инфраструктура;  виртуальная машина;  аппаратное обеспечение;  СПО |
| 13.6 | Угроза недобросовестного исполнения обязательств поставщиками облачных услуг | внешний нарушитель с низким потенциалом | ИС;  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 | ИС, иммигрированная в облако;  облачная система |
| 13.9 | Угроза неконтролируемого роста числа виртуальных машин | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | облачная система;  консоль управления облачной инфраструктурой;  облачная инфраструктура |
| 13.10 | Угроза некорректной реализации политики лицензирования в облаке | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО;  ППО;  сетевое ПО |
| 13.11 | Угроза неопределенности в распределении ответственности между ролями в облаке | внешний нарушитель с низким потенциалом;  внутренний нарушитель с низким потенциалом | СПО |
| 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 | СПО;  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;  ИС, иммигрированная в облако |
| 13.17 | Угроза потери и утечки данных, обрабатываемых в облаке | внутренний нарушитель с низким потенциалом | СПО;  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 | ИС, иммигрированная в облако;  СПО;  ППО;  сетевое ПО |
| 13.20 | Угроза привязки к поставщику облачных услуг | внутренний нарушитель с низким потенциалом | ИС, иммигрированная в облако;  СПО;  сетевое ПО;  сетевой трафик;  объекты файловой системы |
| 13.21 | Угроза приостановки оказания облачных услуг вследствие технических сбоев | - | СПО;  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 суперкомпьютера | 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;  СПО |
| 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 | ИС;  сетевой узел;  носитель информации;  объекты файловой системы;  учетные данные пользователя;  образ виртуальной машины |
| 15.2 | Угроза нарушения изоляции пользовательских данных внутри виртуальной машины | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | виртуальная машина;  гипервизор |
| 15.3 | Угроза нарушения технологии обработки информации 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 | ИС;  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 |
| 15.12 | Угроза ошибки обновления гипервизора | внутренний нарушитель с низким потенциалом | СПО;  гипервизор |
| 15.13 | Угроза перехвата управления гипервизором | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО;  гипервизор;  консоль управления гипервизором |
| 15.14 | Угроза перехвата управления средой виртуализации | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | ИС;  СПО |
| 15.15 | Угроза нарушения доверенной загрузки виртуальных серверов ИС, перехват загрузки | - | - |
| 15.16 | Угроза нарушения целостности конфигурации виртуальных серверов - подмена (искажение) образов (данных и оперативной памяти) | - | - |
| 15.17 | Угроза несанкционированного доступа к консоли управления виртуальной инфраструктурой | - | - |
| 15.18 | Угроза несанкционированного доступа к виртуальному серверу ИС, в том числе несанкционированное сетевое подключение и проведение сетевых атак на виртуальный сервер ИС | - | - |
| 15.19 | Угроза несанкционированного удаленного доступа 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 (ее компонентам), виртуальным машинам, объектам внутри них | - | - |
| 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 ИС неучтенных машинных носителей | - | - |
| 16.8 | Угроза подключения к ИС 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 | - | - |
| 16.13 | Угроза встраивания программно-аппаратных закладок в машинные носители | - | - |
| 16.14 | Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | - | - |
| 16.15 | Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | - | - |
| 16.16 | Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | - | - |
| 16.17 | Угроза передачи информации (ее фрагментов) 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) программного обеспечения и оборудования | | |
| 17.1 | Угроза внедрения вредоносного кода в BIOS | внутренний нарушитель с высоким потенциалом | микропрограммное и аппаратное обеспечение;  BIOS/UEFI |
| 17.2 | Угроза изменения компонентов системы | внутренний нарушитель с низким потенциалом | ИС;  сервер;  рабочая станция;  виртуальная машина;  СПО;  ППО;  аппаратное обеспечение |
| 17.3 | Угроза исчерпывания запаса ключей, необходимых для обновления BIOS | внешний нарушитель со средним потенциалом | микропрограммное обеспечение;  BIOS/UEFI |
| 17.4 | Угроза установки на мобильные устройства вредоносных (уязвимых) программных продуктов | - | - |
| 17.5 | Угроза запуска (установки) вредоносного (шпионского, неразрешенного) программного обеспечения и (или) его обновлений | - | - |
| 17.6 | Установка программного обеспечения, содержащего известные уязвимости | - | - |
| 17.7 | Установка нелицензионного программного обеспечения | - | - |
| 17.8 | Угроза ошибочного запуска (установки) программного обеспечения | - | - |
| 17.9 | Угроза неправильной установки программного обеспечения | - | - |
| 17.10 | Угроза автоматического запуска вредоносного (шпионского, неразрешенного) программного обеспечения при запуске ОС и (или) обновлений программного обеспечения | - | - |
| 17.11 | Угроза удаленного запуска (установки) вредоносного (шпионского, неразрешенного) программного обеспечения | - | - |
| 17.12 | Угроза несанкционированного запуска программного обеспечения в нерабочее время | - | - |
|  | 18. Угрозы физического доступа к компонентам ИС | | |
| 18.1 | Угроза преодоления физической защиты | внешний нарушитель со средним потенциалом | сервер;  рабочая станция;  носитель информации;  аппаратное обеспечение |
| 18.2 | Угроза физического выведения из строя средств хранения, обработки и (или) ввода (вывода, передачи) информации | внешний нарушитель с низким потенциалом | сервер;  рабочая станция;  носитель информации;  аппаратное обеспечение |
| 18.3 | Угроза хищения средств хранения, обработки и (или) ввода (вывода, передачи) информации | внешний нарушитель с низким потенциалом | сервер;  рабочая станция;  носитель информации;  аппаратное обеспечение |
| 18.4 | Угроза несанкционированного доступа к СКЗИ | - | - |
| 18.5 | Угроза нарушения функционирования накопителя на жестких магнитных дисках и других систем хранения данных | - | - |
| 18.6 | Угроза доступа к системам обеспечения, их повреждения | - | - |
| 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 и прикладном программном обеспечении, средствах защиты информации, средствах криптографической защиты информации, аппаратных компонентах информационной системы и микропрограммном обеспечении | | |
| 19.1 | Угроза анализа криптографических алгоритмов и их реализации | внешний нарушитель со средним потенциалом | метаданные;  СПО |
| 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 прерывания канала связи с контрольными датчиками | внешний нарушитель с высоким потенциалом;  внутренний нарушитель с низким потенциалом | СПО |
| 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 программного обеспечения BIOS | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | микропрограммное обеспечение;  BIOS/UEFI |
| 19.13 | Угроза перехвата (исключения) сигнала из привилегированного блока функций | внешний нарушитель со средним потенциалом;  внутренний нарушитель со средним потенциалом | СПО |
| 19.14 | Угроза наличия механизмов разработчика | внутренний нарушитель со средним потенциалом | ПО;  ТС |
| 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 | СПО;  сетевое ПО;  сетевой трафик |
| 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 | ИС;  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 | ППО;  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 к ИС с использованием протоколов сетевого доступа к файловым системам | - | - |
| 20.16 | Угроза отсутствия механизмов реагирования (блокирования) атак (вторжений) | - | - |
| 20.17 | Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак (вторжений) | - | - |
| 20.18 | Угроза отсутствия системы анализа сетевого трафика между сегментами ИС 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 ИС с использованием технологии удаленного доступа | - | - |
| 20.24 | Угроза использования неконтролируемых сетевых протоколов для модификации (перехвата) управления ИС | - | - |
| 20.25 | Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | - | - |
| 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 ИС | - | - |
| 20.30 | Отсутствие контроля соединений между СВТ ИС | - | - |
| 20.31 | Угроза несанкционированного доступа к средствам управления информационными потоками | - | - |
| 20.32 | Угроза отсутствия (неиспользования) средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации | - | - |
| 20.33 | Угроза отсутствия средств анализа сетевого трафика на наличие вредоносного ПО | - | - |
| 20.34 | Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны |  |  |
|  | 21. Угрозы инженерной инфраструктуре | | |
| 21.1 | Угрозы сбоев в сети электропитания | - | - |
| 21.2 | Угроза выхода из строя ТС в результате нарушения климатических параметров работы | - | - |
| 21.3 | Угрозы нарушения схем электропитания | - | - |
| 21.4 | Угрозы, связанные с отсутствием заземления (неправильным заземлением) | - | - |
|  | 22. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности | | |
| 22.1 | Угроза отсутствия системы регистрации событий информационной безопасности | - | - |
| 22.2 | Угроза автоматического удаления (затирания) событий информационной безопасности новыми событиями | - | - |
| 22.3 | Угроза переполнения журналов информационной безопасности | - | - |
| 22.4 | Угроза отсутствия централизованной подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | - | - |
| 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, СЗИ | - | - |
| 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 информационной безопасности | - | - |
| 22.14 | Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | - | - |
|  | 23. Угрозы, связанные с контролем защищенности информационной системы | | |
| 23.1 | Угроза отсутствия контроля за уязвимостями ИС, ее компонентами, наличием неразрешенного программного обеспечения | - | - |
| 23.2 | Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности ИС | - | - |
| 23.3 | Угроза установки программного обеспечения (обновлений) без проведения анализа уязвимостей | - | - |
| 23.4 | Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ, с учетом новых угроз безопасности информации | - | - |
| 23.5 | Угроза отсутствия анализа изменения настроек ИС, ее компонентов, в том числе СЗИ, 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 | ППО;  сетевое ПО |
| 24.3 | Угроза перехвата данных | - | - |
| 24.4 | Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | - | - |
| 24.5 | Угроза перехвата данных с сетевых портов | - | - |
| 24.6 | Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа | - | - |

**Список использованных сокращений**

|  |  |  |
| --- | --- | --- |
| БД | - | база данных |
| ВТСС | - | вспомогательные технические средства и системы |
| ВЧ | - | высокочастотный |
| ИВК | - | информационно-вычислительный комплекс |
| ИС | - | информационная система |
| НСД | - | несанкционированный доступ |
| ОС | - | операционная система |
| ПАК | - | программно-аппаратный комплекс |
| ПДн | - | персональные данные |
| ПО | - | программное обеспечение |
| ППО | - | прикладное программное обеспечение |
| ПЭМИН | - | побочные электромагнитные излучения и наводки |
| СВТ | - | средства вычислительной техники |
| СЗИ | - | средства защиты информации |
| СКЗИ | - | средство криптографической защиты информации |
| СПО | - | системное программное обеспечение |
| ТС | - | технические средства |
| УБПДн | - | угрозы безопасности персональных данных |
| BIOS | - | базовая система ввода-вывода |
| HTTP cookies | - | фрагмент данных, отправленный веб-сервисом и хранимый в информационной системе |
| UEFI | - | унифицированный интерфейс расширяемой прошивки |

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