ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОРДОВИЯ

П О С Т А Н О В Л Е Н И Е

от 07.05.2018 № 289

г. Саранск

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

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, Правительство Республики Мордовия **п о с т а н о в л я е т:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, согласно приложению.

2. Исполнительным органам государственной власти Республики Мордовия и подведомственным им организациям определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных, руководствуясь настоящим постановлением.

3. Рекомендовать органам местного самоуправления муниципальных районов в Республике Мордовия и городского округа Саранск, подведомственным им организациям и организациям, в уставном (складочном) капитале которых доля (вклад) Республики Мордовия и (или) муниципальных образований в Республике Мордовия составляет 50% (пятьдесят процентов) и более, и расположенным на территории Республики Мордовия:

Тип. ИМУ. Зак. 1460–2000.

– определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных;

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

4. Настоящее постановление вступает в силу со дня его официального опубликования.

Председатель Правительства Республики Мордовия **В. Сушков**

Правительство Республики Мордовия Аппарат Секретариат № 1

Приложение
к постановлению Правительства
Республики Мордовия
от 7 мая 2018 г. № 289

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных

1. Общие положения

1. Настоящий документ определяет перечень угроз безопасности персональных данных (далее – УБ ПДн), актуальных при обработке персональных данных (далее - ПДн) в информационных системах персональных данных (далее – ИСПДн), эксплуатируемых органами исполнительной власти Республики Мордовия, и (или) подведомственными им организациями, и (или) организациями, в уставном (складочном) капитале которых доля (вклад) Республики Мордовия составляет 50% (пятьдесят процентов) и более, и расположенными на территории Республики Мордовия (далее – соответственно Органы, Организации), при осуществлении ими соответствующих видов деятельности, с учетом содержания ПДн, характера и способов их обработки.

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

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

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

4. При определении УБ ПДн, актуальных при обработке ПДн в используемых ИСПДн, и совокупности предположений о возможностях нарушителя, которые могут использоваться при создании, подготовке и проведении атак, Органы и Организации применяют с учетом категории

ИСПДн, условий и особенностей функционирования ИСПДн, характера и способов обработки ПДн в ИСПДн:

1) типовые возможности нарушителей безопасности информации и направления атак, приведенные в приложении 2 к настоящему документу;

2) группы актуальных УБ ПДн в ИСПДн, приведенные в разделе 6 настоящего документа;

3) расширенный перечень УБ ПДн в ИСПДн, приведенный в приложении 1 к настоящем документу, и согласно действующим методикам определения актуальных угроз безопасности информации осуществляют определение актуальных УБ ПДн.

5. Настоящий документ применяется совместно с банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru), а также базовыми и типовыми моделями угроз безопасности информации в информационных системах различных классов и типов, разрабатываемых ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

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

7. В настоящем документе дано описание:

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

8. В настоящем документе используются термины и понятия, установленные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных,

утвержденной заместителем директора ФСТЭК России 14 февраля 2008 г., а также:

«ЗСПД» – Защищенная сеть передачи данных исполнительных органов государственной власти и органов местного самоуправления Республики Мордовия. Подключение к данной сети ее участников осуществляется с применением аппаратно-программного комплекса шифрования, обеспечивающего идентификацию и аутентификацию пользователей, доверенную загрузку, контроль целостности программной среды, ведение журнала регистрации событий, ведение системного журнала безопасности. Данный комплекс: имеет сертификат соответствия ФСТЭК России, подтверждающий соответствие требованиям руководящих документов по 3 уровню контроля на отсутствие недекларированных возможностей; может использоваться для создания автоматизированных систем до класса защищенности 1В включительно и при создании ИСПДн до 1 класса включительно (сертификат соответствия ФСБ России, подтверждающий соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3 и возможность применения для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну). Данная сеть позволяет обеспечить защиту ИСПДн всех уровней и классов защищенности уже на стадии создания;

«СВТ» – средства вычислительной техник;

«АРМ» – автоматизированное рабочее место пользователя;

«НСД» – несанкционированный доступ;

«НДВ» – недекларированные возможности;

«СПО» – системное программное обеспечение;

«ППО» – прикладное программное обеспечение;

«СЗИ» – средства защиты информации;

«СКЗИ» – средства криптографической защиты информации.

2. Владельцы и операторы ИСПДн, сети передачи данных

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

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

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

сетям связи общего пользования (сетям международного информационного обмена) и расположенное за пределами территории Органа (Организации).

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

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

- оптоволоконные каналы связи операторов связи (провайдеров);
- проводные каналы связи операторов связи (провайдеров);

2) сетям Органов, Организаций и организаций (предприятий, учреждений), расположенных на территории Российской Федерации. Подключение к данным сетям осуществляется в соответствии с разработанными регламентами взаимодействия. Органы исполнительной власти Республики Мордовия имеют подключение к ЗСПД посредством защищенных каналов связи;

3) иным сетям, взаимодействие с которыми организовано Органами и Организациями с целью осуществления своих полномочий.

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

3. Объекты защиты и технологии обработки ПДн в ИСПДн

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

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

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

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

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

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

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

1) АРМ с различными уровнями доступа (правами). АРМ представляет собой программно-аппаратный комплекс, позволяющий осуществлять доступ пользователей к ИСПДн и предназначенный для локальной обработки информации;

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

3) Серверное оборудование, которое представляет 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.)), предназначенный для обработки и консолидированного хранения данных ИСПДн. Серверное оборудование может быть представлено АРМ, выполняющими функции сервера;

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

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

16. Ввод ПДн в ИСПДн в Органах и Организациях осуществляется как с бумажных носителей, так и с электронных носителей информации, также ПДн могут быть введены в ИСПДн операторами или субъектами ПДн самостоятельно. Выводятся ПДн из ИСПДн как в электронном, так и в бумажном виде с целью их хранения и (или) передачи третьим лицам.

4. ИСПДн

17. С целью осуществления своих полномочий Органами и Организациями обрабатываются все категории ПДн. Состав ПДн, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции),

совершаемые с ПДн в ИСПДн, определяются Органом (Организацией), являющимся оператором ИСПДн.

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

19. ИСПДн подразделяются на:

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

20. ИСПДн и ее компоненты расположены в пределах Российской Федерации.

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

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

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

23. В рамках ИСПДн возможны сбор (хранение), систематизация, уточнение (обновление, изменение), использование, распространение (в том числе передачу), печать и передача ПДн.

4.1. Информационно-справочные ИСПДн

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

25. К основным информационно-справочным ИСПДн относятся:

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

26. Официальные порталы (сайты) Органов и Организаций. Данные ИСПДн содержат сведения о деятельности Органов и Организаций, в том числе сведения, подлежащие обязательному опубликованию в данных ИСПДн в соответствии с действующим законодательством.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

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

Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане Российской Федерации (далее – РФ) и иностранные граждане.

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

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

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

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

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

Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

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

Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане РФ и иностранные граждане.

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

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

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

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

28. Закрытые порталы для нескольких групп участников Органов и (или) Организаций. Данные ИСПДн содержат сведения, предоставляемые ограниченному круг лиц из числа Органов и (или) Организаций в соответствии с функциями и полномочиями Органов (Организаций).

Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

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

Типы субъектов, ПД которых могут подлежать обработке в ИСПДн: сотрудники Органов и (или) Организаций.

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

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

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

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

29. Республиканский портал государственных и муниципальных услуг (функций). Данная ИСПДн содержит социально значимую информацию и

сведения, необходимые для получения гражданами государственных и муниципальных услуг в том числе в электронном виде.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные.

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

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

Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане РФ и иностранные граждане, лица без гражданства.

Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации), и (или) на серверном оборудовании иного Органа (Организации) в пределах его контролируемой зоны

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

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

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

4.2. Сегментные ИСПДн

30. Сегментные ИСПДн представляют собой сегменты федеральных ИСПДн, создаются и эксплуатируются на уровне Республики Мордовия в соответствии с рекомендациями федеральных органов исполнительной власти и используются для сбора, обработки, свода данных на уровне Республики Мордовия и передачи их на федеральный уровень, и обратно, при этом цели и задачи создания (модернизации), эксплуатации данных ИСПДн определяются на федеральном уровне. Данные ИСПДн предназначены для реализации

полномочий федеральных органов власти и исполнения функций Органов (Организаций).

31. К основным сегментным ИСПДн относятся:

- государственная автоматизированная информационная система «Управление»;

- автоматизированная информационная система «Республиканский реестр государственных и муниципальных услуг (функций)» - региональный фрагмент общефедеральной системы;

- автоматизированная информационная система «Федеральный портал малого и среднего предпринимательства».

32. Обработке в ИСПДн могут подлежать все категории ПДн. Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Органов (Организаций) в специализированных программах и (или) посредством веб-интерфейса, и в отдельных случаях гражданами РФ и иностранными гражданами в режиме веб-интерфейса (с ограниченными правами доступа).

33. Типы субъектов ПДн, которые могут подлежать обработке в ИСПДн: граждане РФ и иностранные граждане.

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

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

- подключенные посредством ЗСПД;

- подключенные с использованием иных каналов связи.

Обмен ПДн с центральным сегментом, находящимся вне контролируемой зоны Органа (Организации) и принадлежащим органу власти (организации) федерального уровня, между региональными сегментами ИСПДн (при наличии) и с иными ИСПДн осуществляется в зависимости от технологии подключения к сетям связи общего пользования (сетям международного информационного обмена):

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

- посредством ЗСПД;

- с использованием иных СЗИ для передачи информации по открытым каналам связи.

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

37. По технологии обработки ИСПДн подразделяются на:

- построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение,

осуществляющее подключение к серверному сегменту, располагающемуся в пределах контролируемой зоны Органа (Организации) и передающему данные на центральный сегмент, или напрямую к центральному сегменту в целях передачи данных;

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

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

ИСПДн, реализованные по технологии «тонкого клиента», подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) электронного сертификата, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) электронного сертификата, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

4.3. Внутриреспубликанские ИСПДн

38. Внутриреспубликанские ИСПДн создаются и эксплуатируются по решению органов государственной власти Республики Мордовия или Органа (Организации) в интересах нескольких Органов (Организаций), при этом цели и задачи создания (модернизации), эксплуатации данных ИСПДн, а также требования к ним определяются на уровне Республики Мордовия или Органа (Организации), соответственно.

39. По выполняемым функциям ИСПДн подразделяются на:

- интеграционные (система межведомственного электронного взаимодействия Республики Мордовия (РСМЭВ));

- многопрофильные (например, Система ведомственного и межведомственного электронного документооборота и автоматизированного делопроизводства; автоматизированная информационная система «Многофункциональные центры предоставления государственных и муниципальных услуг Республики Мордовия»; автоматизированная информационная система «Республиканский реестр государственных и

муниципальных услуг (функций)»; автоматизированная информационная система «Республиканский портал государственных и муниципальных услуг (функций)»; Региональная система обработки единой социальной электронной карты жителя Республики Мордовия);

- ИСПДн для Органов и Организаций, и иных организаций Республики Мордовия.

40. ИСПДн интеграционные отвечают следующим признакам:

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

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные;
- общедоступные;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: граждане РФ и иностранные граждане;

5) Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа (Организации);

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

- подключенные посредством ЗСПД;
- подключенные с использованием иных каналов связи;

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

- без подключения (передача ПДн осуществляется с использованием машинных носителей);
- посредством ЗСПД;
- с использованием иных СЗИ для передачи информации по открытым каналам связи;

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

41. ИСПДн многопрофильные отвечают следующим признакам:

1) Данная ИСПДн предназначена для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции,

обращений граждан, обеспечения доступа к электронным документам и т.п. в Органах;

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные;
- общедоступные;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: граждане РФ и иностранные граждане;

5) Структура ИСПДн: локальная или распределенная, функционирующая в контролируемой зоне Органа (Организации);

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

- подключенные посредством ЗСПД;
- подключенные с использованием иных каналов связи;

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

- посредством ЗСПД;
- с использованием сторонних СКЗИ;

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

42. ИСПДн для Органов и Организаций, и иных организаций Республики Мордовия отвечают следующим признакам:

1) Данные ИСПДн предназначены для автоматизации совместной деятельности Органов, Организаций и иных организаций Республики Мордовия;

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- иные;
- общедоступные;

3) Режим обработки ПДн в ИСПДн: многопользовательский, ИСПДн предусматривает разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Органов (Организаций) и организациями Республики Мордовия в специализированных программах в режиме веб-интерфейса;

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органов (Организаций) и организаций Республики Мордовия;

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

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

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

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

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

43. По архитектуре внутриреспубликанские ИСПДн подразделяются на:

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

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

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

По технологии обработки ИСПДн подразделяются на:

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

центральный сегмент.

ИСПДн, реализованные по технологии «тонкого клиента», подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

2) Централизованные ИСПДн, которые делятся на сегменты (центральный и периферийный).

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

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

По технологии обработки ИСПДн подразделяются на:

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

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

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

ИСПДн, реализованные по технологии тонкого клиента, подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

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

4.4. Ведомственные ИСПДн

44. Ведомственные ИСПДн создаются (эксплуатируются) по решению Органа (Организации) в их интересах и интересах подведомственных им организаций, цели и задачи создания (модернизации), эксплуатации которых определяются Органом (Организацией). Ведомственные ИСПДн предназначены для осуществления функций Органов (Организаций).

45. К основным ведомственным ИСПДн относятся:

- комплексная медицинская информационная система Министерства здравоохранения Республики Мордовия;
- автоматизированная информационная система «Региональный сегмент ГИС контингент»;
- автоматизированная информационная система «Управление транспортом»;
- программно-технологический комплекс «Система обработки информации службы занятости населения»;
- автоматизированная информационная система «Электронный социальный регистр населения Республики Мордовия»;
- автоматизированная информационная система «Организация делопроизводства мирового судьи»;
- многоуровневая автоматизированная интегрированная система «ЗАГС»;
- программный комплекс Бюджет КС\Web;
- автоматизированная информационная система «Охотничий билет».

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

- специальные;
- иные.

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

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

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

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

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

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

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

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

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

52. По архитектуре ведомственные ИСПДн подразделяются на:

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

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

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

По технологии обработки ИСПДн подразделяются на:

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

пределах контролируемой зоны Органа (Организации) и передающем данные на центральный сегмент.

ИСПДн, реализованные по технологии «тонкого клиента», подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

2) Централизованные ИСПДн, которые делятся на сегменты (центральный и периферийный).

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

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

По технологии обработки ИСПДн подразделяются на:

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

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

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

ИСПДн, реализованные по технологии «тонкого клиента», подразделяются на:

- реализованные посредством веб-интерфейса с применением веб-браузера и с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

- реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля, и (или) сертификата электронной подписи в соответствии с Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об

электронной подписи»;

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

4.5. Служебные ИСПДн

53. Служебные ИСПДн создаются (эксплуатируются) по решению Органа (Организации) и в их интересах, цели и задачи создания (модернизации), эксплуатации служебных ИСПДн определяются Органом (Организацией), и используются для автоматизации определённой области деятельности или типовой деятельности, неспецифичной относительно полномочий конкретного Органа (Организации).

54. К основным служебным ИСПДн относятся:

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

55. ИСПДн бухгалтерского учета и управления финансами обладают следующими признаками:

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

2) Обработке в ИСПДн подлежат иные категории ПДн;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн;

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

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

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

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

- с использованием сторонних СКЗИ;

8) СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование;

9) По технологии обработки ИСПДн подразделяются на:

- построенные по технологии «толстого клиента»: на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая хранится на серверном сегменте (сервере / АРМ, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Органа (Организации);

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

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

56. ИСПДн кадрового учета и управления персоналом обладают следующими признаками:

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

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;

- иные;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане Российской Федерации, устанавливающие (имеющие) трудовые отношения с Органом (Организацией);

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

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

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

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

7) СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование;

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

57. ИСПДн пенсионного фонда и налоговых служб обладают следующими признаками:

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

2) Обработке в ИСПДн подлежат иные категории ПДн;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн;

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

- без подключения (передача ПДн осуществляется с использованием

машинных носителей);

- подключенные посредством ЗСПД;

- подключенные с использованием иных каналов связи;

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

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

- с использованием сторонних СКЗИ;

8) СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование;

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

58. ИСПДн документооборота и делопроизводства обладают следующими признаками:

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

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;

- иные;

- общедоступные;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане РФ и иностранные граждане;

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

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

- подключенные с использованием иных каналов связи;

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

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

8) СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование;

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

59. ИСПДн поддерживающие обладают следующими признаками:

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

2) Категории ПДн, которые могут подлежать обработке в ИСПДн:

- специальные;
- иные;
- общедоступные;

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

4) Типы субъектов, ПДн которых могут подлежать обработке в ИСПДн: сотрудники Органа (Организации), являющегося оператором ИСПДн, граждане РФ и иностранные граждане;

5) Структура ИСПДн: локальная, функционирующая в контролируемой зоне Органа (Организации);

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

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

7) Передача ПДн в иные ИСПДн не осуществляется;

8) СВТ, участвующие в обработке: АРМ, серверное оборудование, сетевое и телекоммуникационное оборудование;

9) По технологии обработки ИСПДн подразделяются на:

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

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

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

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

5. УБ ПДн, выявленные при функционировании ИСПДн

60. Источники УБ ПДн.

Источниками УБ ПДн в ИСПДн выступают:

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

61. Носитель вредоносной программы.

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

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

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

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

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные

атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

62. Аппаратная закладка.

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

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

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

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

63. Нарушитель.

Нарушителем является субъект доступа, осуществляющий доступ к информации с нарушением правил разграничения доступа, а также лицо, осуществляющее перехват информации по техническим каналам утечки. Нарушитель рассматривается как один из источников угроз НСД в ИСПДн и утечки информации по техническим каналам.

В результате действий нарушителя может быть нанесен ущерб безопасности обрабатываемой в ИСПДн информации, то есть могут быть нарушены ее свойства безопасности, такие как конфиденциальность, целостность (достоверность) и доступность.

Описание потенциальных нарушителей ИСПДн необходимо для формирования перечня источников угроз и является неотъемлемой частью процесса составления полного перечня потенциально реализуемых угроз в рассматриваемых ИСПДн.

По наличию права постоянного или разового доступа в контролируемую зону ИСПДн нарушители подразделяются на два типа:

- внешние нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- внутренние нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

64. Внешний нарушитель.

Внешними нарушителями могут быть:

- разведывательные службы государств;
- криминальные структуры;
- конкуренты (конкурирующие организации);
- недобросовестные партнеры;
- внешние субъекты (физические лица, в том числе бывшие сотрудники организации).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Разведывательные службы государств и криминальные структуры не имеют мотивации осуществления деятельности, связанной с нарушением характеристик безопасности информации.

Конкуренты (конкурирующие организации) как потенциальные нарушители информационной безопасности ИСПДн не рассматриваются по причине отсутствия таковых.

Недобросовестные партнеры не рассматриваются в качестве потенциальных нарушителей информационной безопасности ИСПДн по причине высокой стоимости работ, по созданию способов и средств атаки на информацию, обрабатываемых в Органах, Организациях.

Таким образом, в качестве внешних нарушителей информационной безопасности ИСПДн имеет смысл рассматривать исключительно внешние субъекты (физические лица, в том числе бывшие сотрудники организации), действующих либо самостоятельно, либо вступивших в сговор между собой.

66. Внутренний нарушитель.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к информации.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к информации. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории, может:

– иметь доступ к фрагментам конфиденциальной информации, распространяющейся по внутренним каналам связи ИСПДн;

– располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;

– располагать именами и вести выявление паролей зарегистрированных пользователей;

– изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

– обладает всеми возможностями лиц первой категории;

– знает, по меньшей мере, одно легальное имя доступа;

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству конфиденциальной информации;

– располагает конфиденциальными данными, к которым имеет доступ.

– его доступ, аутентификация и права по доступу к некоторому подмножеству конфиденциальной информации должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИС, осуществляющие удаленный доступ к конфиденциальной информации по локальным и (или) распределенным информационным системам.

Лицо этой категории:

– обладает всеми возможностями лиц первой и второй категорий;

– располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;

– имеет возможность прямого (физического) доступа к фрагментам технических средств ИС.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты

объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

– обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты конфиденциальной информации, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

67. При моделировании принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

– работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;

– нарушитель скрывает свои несанкционированные действия от других сотрудников;

– несанкционированные действия данной группы нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

– легальный доступ посторонних лиц (не принадлежащих к указанным категориям) в помещения, где размещены компоненты ИСПДн, и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

– за деятельностью сотрудников сторонних организаций, имеющих доступ в контролируемую зону, осуществляется контроль;

– внутренние нарушители обладают всеми ресурсами и возможностями для осуществления атак, присущими внешнему нарушителю.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

68. На лиц категорий 4, 5 и 6, указанных в пункте 66 возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн, что позволяет отнести их к группе привилегированных пользователей (группе администраторов). Администраторы потенциально могут реализовывать угрозы информационной безопасности, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных автоматизированных системах, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз информационной безопасности. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

Наличие привилегированных пользователей требует реализации необходимых организационных мер для снижения риска информационной безопасности. Должны применяться следующие организационные меры:

– регламентированы и внедрены процедуры управления доступом в контролируемую зону, к аппаратным и программным средствам обработки и защиты информации;

– определены должности сотрудников (роли), которым предоставляется привилегированные права доступа к информации ограниченного доступа;

– в должностные обязанности привилегированных пользователей включены обязанности в области защиты информации;

– сформированы требования к кандидатам на трудоустройство на должности привилегированных пользователей;

– определены процедуры отбора и проверок кандидатов на трудоустройство на должности привилегированных пользователей;

– определены процедуры оформления приема сотрудников на должности привилегированных пользователей;

– определены процедуры увольнения сотрудников, занимавших должности привилегированных пользователей;

– организовано обучение и инструктажи в области защиты информации;

– определены механизмы стимулирования и поощрения различного характера (в т.ч. финансового);

– организованы, документально оформлены и внедрены принципы разграничения полномочий и двойного управления для решения задач, связанных с администрированием программных и технических средств, в том числе средств обеспечения информационной безопасности;

– определены процедуры реагирования на нарушения информационной безопасности;

– определены процедуры контроля выполнения требований;

– определена ответственность за нарушения информационной безопасности.

В случае если указанные меры руководством не предпринимаются, привилегированных пользователей (группу администраторов) следует рассматривать в качестве потенциальных нарушителей. При этом вероятность реализации практически любой существующей угрозы следует признавать высокой, а, следовательно, саму угрозу – актуальной.

Предполагается, что в число лиц категорий 4,5 и 6 ИСПДн Органов, Организаций будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Лица первой категории ввиду принятых организационных мер на территории учреждения не рассматриваются.

Лица категории 7 и 8 не имеют мотивации осуществления деятельности, связанной с нарушением характеристик безопасности информации и не рассматриваются в качестве потенциальных нарушителей информационной безопасности ИСПДн по причине высокой стоимости работ, по созданию способов и средств атаки на информацию, обрабатываемой в Органах, Организациях.

Предполагается, что лица категорий 2 и 3 относятся к вероятным внутренним нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предполагается, что возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей исключена ввиду применения в Органах, Организациях организационно-технических и кадрово-режимных мер.

69. Основные УБ ПДн в ИСПДн.

Основными группами УБ ПДн в ИСПДн являются:

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

программном обеспечении;

- угрозы неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

- угрозы стихийных бедствий.

6. Актуальные УБ ПДн в ИСПДн

70. Актуальные угрозы безопасности в информационно-справочных ИСПДн:

1) Официальные порталы (сайты) Органов и Организаций:

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

2) Информационные порталы (сайты):

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

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

3) Закрытые порталы для нескольких групп участников Органов и (или) Организаций:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;

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

4) Республиканский портал государственных и муниципальных услуг (функций):

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

компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

71. Актуальные угрозы безопасности в служебных ИСПДн:

1) ИСПДн бухгалтерского учета и управления финансами:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

- угрозы нарушения доступности информации;

- угрозы нарушения целостности информации;

- угрозы, не являющиеся атаками;

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

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

- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;

- угрозы ошибочных/деструктивных действий лиц;

- угрозы нарушения конфиденциальности;

- угрозы программно-математических воздействий;

- угрозы, связанные с использованием технологий виртуализации;

- угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

2) ИСПДн кадрового учета и управления персоналом:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

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

3) ИСПДн пенсионного фонда и налоговых служб:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с нарушением правил эксплуатации машинных

носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

- угрозы нарушения доступности информации;

- угрозы нарушения целостности информации;

- угрозы, не являющиеся атаками;

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

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

- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;

- угрозы ошибочных/деструктивных действий лиц;

- угрозы нарушения конфиденциальности;

- угрозы программно-математических воздействий;

- угрозы, связанные с использованием технологий виртуализации;

- угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

4) ИСПДн поддерживающие:

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

72. Актуальные угрозы безопасности в ведомственных ИСПДн:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;

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

73. Актуальные угрозы безопасности в внутриреспубликанских ИСПДн:

1) ИСПДн интеграционные:

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

компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

-угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

2) ИСПДн многопрофильные:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

- угрозы нарушения доступности информации;

- угрозы нарушения целостности информации;

- угрозы, не являющиеся атаками;

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

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

- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;

- угрозы ошибочных/деструктивных действий лиц;

- угрозы нарушения конфиденциальности;

- угрозы программно-математических воздействий;

- угрозы, связанные с использованием технологий виртуализации;

- угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

3) ИСПДн для Органов и Организаций, и иных организаций (предприятий, учреждений) Республики Мордовия:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

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

4) Сегментные ИСПДн:

- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;

- угрозы, связанные с использованием технологий виртуализации;

- угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

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

7. Меры, направленные на минимизацию УБ ПДн в ИСПДн

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

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

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

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

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

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

- приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

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

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

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

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

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

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

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

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

75. Реализация правовых, организационных и технических мер, направленных на минимизацию УБ ПДн в ИСПДн, осуществляется специалистами по информационной безопасности (специалистами по защите

(технической защите) информации) Органов (Организаций), ответственными за планирование, организацию и реализацию мероприятий по обеспечению информационной безопасности в Органе (Организации).

Приложение 1
к Угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных

Расширенный перечень угроз безопасности персональных данных в информационной системе персональных данных

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
I. Угрозы утечки информации по техническим каналам			
1. Угрозы утечки акустической информации			
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
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
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
4.	Использование средств ВЧ-	внешний	файлы БД системы,

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	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)	нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	файлы сканов документов в виде электромагнитного излучения
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
6.	Применение акустооптических модуляторов на базе волоконно-оптической, находящихся в поле акустического сигнала («оптических микрофонов»)	внешний нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	файлы БД системы, файлы сканов документов в виде электромагнитного излучения
2. Угрозы утечки видовой информации			
7.	Визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИС	внешний нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	файлы БД системы, файлы сканов документов в виде электромагнитного излучения
8.	Визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ,	внешний нарушитель с высоким потенциалом, внутренний	файлы БД системы, файлы сканов документов в виде электромагнитного излучения

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	ИВК, входящих в состав ИС	нарушитель с высоким потенциалом	
9.	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
3. Угрозы утечки информации по каналам ПЭМИН			
10.	Применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (программно-аппаратный комплекс (далее – ПАК), сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)	внешний нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	файлы БД системы, файлы сканов документов в виде электромагнитного излучения
11.	Применение токосъемников для регистрации наводок информативного сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений	внешний нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	файлы БД системы, файлы сканов документов в виде электромагнитного излучения
12.	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
13.	Применение специальных средств регистрации	внешний нарушитель с	файлы БД системы, файлы сканов

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	радиоизлучений, формируемых в результате ВЧ-облучения ТС ИС, в которых проводится обработка информативных сигналов - параметрических каналов утечки	высоким потенциалом, внутренний нарушитель с высоким потенциалом	документов в виде электромагнитного излучения
II. Угрозы использования штатных средств ИС с целью совершения НСД к информации			
14.	Угроза некорректного использования функционала программного обеспечения	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО, микропрограммное обеспечение, аппаратное обеспечение
15.	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
16.	Угроза несанкционированного изменения аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, объекты файловой системы, учётные данные пользователя, реестр
17.	Угроза несанкционированного использования привилегированных функций BIOS	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
18.	Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ		
III. Угрозы нарушения доступности информации			
19.	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
20.	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	грид-система, сетевой трафик
21.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	гипервизор
22.	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные
23.	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	внутренний нарушитель с низким потенциалом	система хранения данных суперкомпьютера

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
24.	Угроза перегрузки грид-системы вычислительными заданиями	внутренний нарушитель с низким потенциалом	ресурсные центры грид-системы
25.	Угроза повреждения системного реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы, реестр
26.	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
27.	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
28.	Угроза утраты вычислительных ресурсов	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	ИС, сетевой узел, носитель информации, СПО, сетевое ПО, сетевой трафик
29.	Угроза вывода из строя/выхода из строя отдельных ТС*		
30.	Угроза вывода из строя незарезервированных		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	ТС/программных средств/каналов связи		
31.	Угроза отсутствия актуальных резервных копий информации*		
32.	Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи*		
33.	Угроза переполнения канала связи вследствие множества параллельных попыток авторизации*		
34.	Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью*		
35.	Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации*		
IV. Угрозы нарушения целостности информации			
36.	Угроза нарушения целостности данных кеша	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевое ПО
37.	Угроза некорректного задания структуры данных транзакции	внутренний нарушитель со средним потенциалом	сетевой трафик, база данных, сетевое ПО
38.	Угроза переполнения целочисленных переменных	внешний нарушитель со средним	СПО, ППО, сетевое ПО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом, внутренний нарушитель со средним потенциалом	
39.	Угроза подмены содержимого сетевых ресурсов	внешний нарушитель с низким потенциалом	ППО, сетевое ПО, сетевой трафик
40.	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	внутренний нарушитель с низким потенциалом	ИС, узлы хранилища больших данных
41.	Угроза сбоя обработки специальным образом изменённых файлов	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	метаданные, объекты файловой системы, СПО
42.	Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ*		
43.	Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности*		
44.	Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми*		
45.	Отсутствие средств централизованного управления		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	за поступающими в информационную систему данными, в том числе незапрашиваемыми		
46.	Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации		
47.	Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей		
48.	Угроза отсутствия контроля за данными, передаваемыми из ИС*		
49.	Отсутствие резервного копирования информации, передаваемой из ИС		
50.	Угроза передачи из ИС недопустимой информации		
51.	Угроза отсутствия контроля за данными вводимыми в систему пользователями*		
52.	Угроза ввода/передачи недостоверных/ошибочных данных*		
53.	Угроза подмены используемых ИС файлов*		
54.	Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты*		
55.	Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения		
56.	Угроза		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	модификации/стирания/удаления данных системы регистрации событий информационной безопасности		
57.	Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ		
58.	Угроза отсутствия контроля целостности информации, обрабатываемой ИС, и ее структуры		
V. Угрозы НДВ в СПО и ППО			
59.	Угроза перебора всех настроек и параметров приложения	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО, микропрограммное обеспечение, реестр
60.	Угроза возникновения ошибок функционирования СПО, реализация недекларированных возможностей системного ПО		
61.	Угроза использования встроенных недекларированных возможностей для получения несанкционированного доступа к ИС		
VI. Угрозы, не являющиеся атаками			
62.	Угроза исчерпания вычислительных ресурсов хранилища больших данных	внутренний нарушитель с низким потенциалом	ИС
63.	Угроза неверного определения формата входных данных, поступающих в хранилище	внутренний нарушитель с низким	хранилище больших данных, метаданные

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	больших данных	потенциалом	
64.	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	внутренний нарушитель с низким потенциалом	рабочая станция, носитель информации, СПО, метаданные, объекты файловой системы, реестр
65.	Угроза неконтролируемого копирования данных внутри хранилища больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные, защищаемые данные
66.	Угроза неконтролируемого уничтожения информации хранилищем больших данных	внутренний нарушитель с низким потенциалом	хранилище больших данных, метаданные, защищаемые данные
67.	Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи		
VII. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации			
68.	Угроза аппаратного сброса пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
69.	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, метаданные, учётные данные пользователя
70.	Угроза обхода некорректно настроенных механизмов аутентификации	внешний нарушитель с низким потенциалом, внутренний	СПО, сетевое ПО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		нарушитель с низким потенциалом	
71.	Угроза программного сброса пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI, СПО
72.	Угроза «кражи» учётной записи доступа к сетевым сервисам	внешний нарушитель с низким потенциалом	сетевое ПО
73.	Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации*		
74.	Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации*		
75.	Угроза получения несанкционированного доступа в результате сбоев/ошибок подсистемы идентификация и аутентификация*		
76.	Угроза получения несанкционированного доступа сторонними лицами, устройствами*		
77.	Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС		
78.	Угрозы авторизации с использованием устаревших, но не отключённых учетных записей*		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
79.	Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа		
80.	Угроза применения только программных методов двухфакторной аутентификации		
81.	Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа		
82.	Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ		
83.	Угроза доступа к ИС неаутентифицированных устройств и пользователей		
84.	Угроза повторного использования идентификаторов в течение как минимум 1 года		
85.	Угроза использования идентификаторов, неиспользуемых более 45 дней		
86.	Угроза раскрытия используемых идентификаторов пользователя в публичном доступе		
87.	Отсутствие управления идентификаторами внешних пользователей		
88.	Угроза использования «слабых»/предсказуемых паролей		
89.	Отсутствие отказоустойчивой		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	централизованной системы идентификации и аутентификации		
90.	Угроза использования пользователями идентичных идентификаторов в разных информационных системах		
91.	Угроза использования неподписанных программных средств		
92.	Угроза запуска несанкционированных процессов и служб от имени системных пользователей		
93.	Угроза отсутствия регламента работы с персональными идентификаторами		
94.	Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей		
95.	Угроза бесконтрольного доступа пользователей к процессу загрузки		
96.	Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования		
VIII. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом			
97.	Угроза воздействия на программы с высокими привилегиями	внешний нарушитель со средним потенциалом, внутренний нарушитель со	ИС, виртуальная машина, сетевое ПО, сетевой трафик

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		средним потенциалом	
98.	Угроза доступа к защищаемым файлам с использованием обходного пути	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы
99.	Угроза доступа к локальным файлам сервера при помощи URL	внешний нарушитель со средним потенциалом	сетевое ПО
100.	Угроза загрузки нештатной ОС	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI
101.	Угроза изменения режимов работы аппаратных элементов компьютера	внутренний нарушитель с высоким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
102.	Угроза изменения системных и глобальных переменных	внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО
103.	Угроза использования альтернативных путей доступа к ресурсам	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевой узел, объекты файловой системы, ППО, СПО
104.	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	внешний нарушитель со средним потенциалом, внутренний	СЗИ, СПО, сетевое ПО, микропрограммное обеспечение, программно-

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		нарушитель с низким потенциалом	аппаратные средства со встроенными функциями защиты
105.	Угроза использования механизмов авторизации для повышения привилегий	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО
106.	Угроза нарушения изоляции среды исполнения BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
107.	Угроза невозможности управления правами пользователей BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI
108.	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	внешний нарушитель с низким потенциалом	сетевое ПО
109.	Угроза неправомерного ознакомления с защищаемой информацией	внутренний нарушитель с низким потенциалом	аппаратное обеспечение, носители информации, объекты файловой системы
110.	Угроза несанкционированного доступа к аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации
111.	Угроза несанкционированного	внешний	сетевой узел,

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	доступа к системе по беспроводным каналам	нарушитель с низким потенциалом	учётные данные пользователя, сетевой трафик, аппаратное обеспечение
112.	Угроза несанкционированного копирования защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	объекты файловой системы, машинный носитель информации
113.	Угроза несанкционированного редактирования реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, использующее реестр, реестр
114.	Угроза несанкционированного создания учётной записи пользователя	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО
115.	Угроза несанкционированного управления буфером	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО
116.	Угроза несанкционированного управления синхронизацией и состоянием	внешний нарушитель со средним	СПО, ППО, сетевое ПО, микропрограммное

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом, внутренний нарушитель со средним потенциалом	обеспечение
117.	Угроза несанкционированного управления указателями	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО
118.	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	внутренний нарушитель с низким потенциалом	СПО, ППО
119.	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, аппаратное обеспечение
120.	Угроза перехвата привилегированного потока	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО
121.	Угроза перехвата привилегированного процесса	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним	СПО, ППО, сетевое ПО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом	
122.	Угроза повышения привилегий	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, сетевое ПО, ИС
123.	Угроза подбора пароля BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI
124.	Угроза подделки записей журнала регистрации событий	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО
125.	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных		ИС, система разграничения доступа хранилища больших данных
126.	Угроза удаления аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, микропрограммное обеспечение, учётные данные пользователя
127.	Угроза «форсированного веб-браузинга»	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО
128.	Угроза эксплуатации цифровой подписи программного кода	внешний нарушитель с	СПО, ППО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		низким потенциалом, внутренний нарушитель с низким потенциалом	
129.	Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя*		
130.	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа*		
131.	Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа*		
132.	Угроза бесконтрольной передачи данных как внутри ИС, так и между ИС*		
133.	Угроза получения дополнительных данных, не предусмотренных технологией обработки*		
134.	Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями*		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
135.	Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий*		
136.	Отсутствие ограничения на количество неудачных попыток входа в информационную систему*		
137.	Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя*		
138.	Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации*		
139.	Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа*		
140.	Угроза подбора идентификационных данных для удаленного доступа к ИС*		
141.	Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа*		
142.	Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств*		
143.	Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	идентификации и авторизации*		
144.	Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств*		
145.	Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем*		
146.	Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа*		
147.	Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации*		
148.	Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей*		
149.	Угроза бесконтрольного доступа к информации неопределенным кругом лиц*		
150.	Угроза получения доступа к данным, не предназначенным для пользователя*		
151.	Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	иных деструктивных целей*		
152.	Угроза модификации, подмены, удаления атрибутов безопасности (меток безопасности) при взаимодействии с иными информационными системами*		
153.	Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств*		
154.	Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты		
155.	Отсутствие отказоустойчивых централизованных средств управления учетными записями		
156.	Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД		
157.	Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации		
158.	Угроза передачи информации разной степени конфиденциальности без разграничения		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	информационных потоков		
159.	Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией		
160.	Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных		
161.	Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными		
162.	Угроза несанкционированного доступа к средствам управления информационными потоками		
163.	Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо		
164.	Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним		
165.	Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа		
166.	Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями		
167.	Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств		
168.	Отсутствие блокирования сеанса пользователя (на мониторе пользователя не должна отображаться информация сеанса пользователя) после времени бездействия 5 минут		
169.	Угроза использования незавершенных сеансов пользователей		
170.	Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа		
171.	Отсутствие автоматизированного мониторинга и контроля удаленного доступа		
172.	Угроза использования уязвимых/незащищенных технологий удаленного доступа		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
173.	Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты		
174.	Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации		
175.	Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации		
176.	Отсутствие контроля за используемыми интерфейсами ввода/вывода		
IX. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС			
177.	Угроза передачи данных по скрытым каналам	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сетевой узел, сетевое ПО, сетевой трафик
178.	Угроза включения в проект не испытанных достоверно компонентов	внутренний нарушитель со средним потенциалом	ПО, ТС, ИС, ключевая система информационной инфраструктуры
179.	Угроза внедрения системной избыточности	внутренний нарушитель со средним	ПО, ИС, ключевая система информационной

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом	инфраструктуры
180.	Угроза ошибок при моделировании угроз и нарушителей информационной безопасности*		
181.	Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности*		
X. Угрозы ошибочных/деструктивных действий лиц			
182.	Угроза подмены действия пользователя путём обмана	внешний нарушитель со средним потенциалом	ППО, сетевое ПО
183.	Угроза «фишинга»	внешний нарушитель с низким потенциалом	рабочая станция, сетевое ПО, сетевой трафик
184.	Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями*		
185.	Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) *		
186.	Создание неконтролируемых		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	точек доступа (лазейки) в систему, для удаленного доступа к ИС*		
187.	Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС*		
188.	Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления*		
189.	Хищение ключей шифрования, идентификаторов и известных паролей*		
190.	Внесение программно-аппаратных закладок в программного - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации*		
191.	Создание методов и средств реализации атак, а также самостоятельное проведение атаки		
192.	Ошибки при конфигурировании и обслуживании модулей/компонентов ИС		
193.	Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений).		
194.	Несанкционированный съем информации, блокирование		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети.		
195.	Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним		
196.	Нарушение правил хранения ключевой информации		
197.	Передача защищаемой информации по открытым каналам связи		
198.	Несанкционированная модификация/уничтожение информации легитимным пользователем		
199.	Копирование информации на незарегистрированный носитель информации, в том числе печать		
200.	Несанкционированное отключение средств защиты		
201.	Угрозы вербовки (социальной инженерии)		
XI. Угрозы нарушения конфиденциальности			
202.	Угроза исследования механизмов работы программы	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО, микропрограммное обеспечение
203.	Угроза исследования приложения через отчёты об ошибках	внешний нарушитель со средним потенциалом, внутренний нарушитель со	СПО, ППО, сетевое ПО, микропрограммное обеспечение

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		средним потенциалом	
204.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, сетевой трафик
205.	Угроза обнаружения хостов	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, сетевой трафик
206.	Угроза определения типов объектов защиты	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, сетевой трафик
207.	Угроза определения топологии вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, сетевой трафик
208.	Угроза получения предварительной информации об объекте защиты	внешний нарушитель со средним потенциалом	сетевой узел, сетевое ПО, сетевой трафик, ППО
209.	Угроза получения сведений о владельце беспроводного устройства	внешний нарушитель с низким потенциалом	сетевой узел, метаданные
210.	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	внешний нарушитель с низким потенциалом	сетевое ПО, сетевой узел
211.	Сканирование сети для изучения логики работы ИС, выявления протоколов, портов*		
212.	Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены*		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
213.	Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) *		
214.	Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты		
215.	Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС		
216.	Угроза получения нарушителем идентификационных данных легальных пользователей ИС		
217.	Разглашение сведений конфиденциального характера		
XII. Угрозы программно-математических воздействий			
218.	Угроза автоматического распространения вредоносного кода в грид-системе	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	ресурсные центры грид-системы
219.	Угроза внедрения кода или данных	внешний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО
220.	Угроза восстановления аутентификационной информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, микропрограммное обеспечение, учётные данные пользователя
221.	Угроза деструктивного изменения конфигурации/среды	внутренний нарушитель с	СПО, ППО, сетевое ПО,

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	окружения программ	низким потенциалом	микропрограммное обеспечение, метаданные, объекты файловой системы, реестр
222.	Угроза избыточного выделения оперативной памяти	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	аппаратное обеспечение, СПО, сетевое ПО
223.	Угроза искажения XML-схемы	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	сетевой узел, сетевое ПО, сетевой трафик
224.	Угроза искажения вводимой и выводимой на периферийные устройства информации	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО, аппаратное обеспечение
225.	Угроза использования слабостей кодирования входных данных	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО, ППО, сетевое ПО, микропрограммное обеспечение, реестр
226.	Угроза межсайтового скриптинга	внешний нарушитель с низким	сетевой узел, сетевое ПО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом	
227.	Угроза межсайтовой подделки запроса	внешний нарушитель со средним потенциалом	сетевой узел, сетевое ПО
228.	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
229.	Угроза перехвата вводимой и выводимой на периферийные устройства информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, аппаратное обеспечение
230.	Угроза подмены резервной копии программного обеспечения BIOS	внутренний нарушитель с низким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
231.	Угроза пропуска проверки целостности программного обеспечения	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО
232.	Угроза заражения компьютера при посещении неблагонадёжных сайтов	внутренний нарушитель с низким потенциалом	сетевой узел, сетевое ПО
233.	Угроза неправомерного шифрования информации	внешний нарушитель с низким потенциалом	объект файловой системы
234.	Угроза скрытного включения вычислительного устройства в	внешний нарушитель с	сетевой узел, сетевое ПО

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	состав бот-сети	низким потенциалом	
235.	Угроза распространения «почтовых червей»	внешний нарушитель с низким потенциалом	сетевое ПО
236.	Внедрение программных закладок/закладок*		
237.	Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа*		
238.	Применение специально созданных программных продуктов для НСД*		
239.	Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения*		
240.	Отсутствие централизованной системы управления средствами антивирусной защиты		
XIII. Угрозы, связанные с использованием облачных услуг			
241.	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	внутренний нарушитель с низким потенциалом	облачная система, виртуальная машина
242.	Угроза злоупотребления доверием потребителей облачных услуг	внешний нарушитель с низким потенциалом	облачная система
243.	Угроза конфликта юрисдикций различных стран	внешний нарушитель с низким потенциалом	облачная система

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
244.	Угроза нарушения доступности облачного сервера	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	облачная система, облачный сервер
245.	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
246.	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	внешний нарушитель с низким потенциалом	ИС, сервер, носитель информации, метаданные, объекты файловой системы
247.	Угроза незащищённого администрирования облачных услуг	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	облачная система, рабочая станция, сетевое ПО
248.	Угроза некачественного переноса инфраструктуры в облако	внешний нарушитель с низким потенциалом	ИС, иммигрированная в облако, облачная система
249.	Угроза неконтролируемого роста числа виртуальных машин	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
250.	Угроза некорректной реализации политики лицензирования в облаке	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, ППО, сетевое ПО
251.	Угроза неопределённости в распределении ответственности между ролями в облаке	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО
252.	Угроза неопределённости ответственности за обеспечение безопасности облака	внешний нарушитель с низким потенциалом	облачная система
253.	Угроза непрерывной модернизации облачной инфраструктуры	внутренний нарушитель со средним потенциалом	облачная инфраструктура
254.	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, облачная система
255.	Угроза общедоступности облачной инфраструктуры	внешний нарушитель со средним потенциалом	объекты файловой системы, аппаратное обеспечение, облачный сервер
256.	Угроза потери доверия к поставщику облачных услуг	внутренний нарушитель со средним	объекты файловой системы, ИС, иммигрированная в

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		потенциалом	облако
257.	Угроза потери и утечки данных, обрабатываемых в облаке	внутренний нарушитель с низким потенциалом	СПО, метаданные, объекты файловой системы
258.	Угроза потери управления облачными ресурсами	внешний нарушитель с высоким потенциалом	сетевой трафик, объекты файловой системы
259.	Угроза потери управления собственной инфраструктурой при переносе её в облако	внутренний нарушитель со средним потенциалом	ИС, иммигрированная в облако, СПО, ППО, сетевое ПО
260.	Угроза привязки к поставщику облачных услуг	внутренний нарушитель с низким потенциалом	ИС, иммигрированная в облако, СПО, сетевое ПО, сетевой трафик, объекты файловой системы
261.	Угроза приостановки оказания облачных услуг вследствие технических сбоев		СПО, аппаратное обеспечение, канал связи
262.	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
XIV. Угрозы, связанные с использованием суперкомпьютерных технологий			
263.	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	внешний нарушитель с низким потенциалом, внутренний нарушитель с	вычислительные узлы суперкомпьютера

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		низким потенциалом	
264.	Угроза несанкционированного доступа к сегментам вычислительного поля	внутренний нарушитель со средним потенциалом	вычислительный узел суперкомпьютера
265.	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
266.	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	внутренний нарушитель с низким потенциалом	вычислительные узлы суперкомпьютера
XV. Угрозы, связанные с использованием технологий виртуализации			
267.	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, учётные данные пользователя, образ виртуальной машины
268.	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	виртуальная машина, гипервизор
269.	Угроза нарушения технологии	внешний	образ виртуальной

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	машины, сетевой узел, сетевое ПО, виртуальная машина
270.	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	ИС, сервер
271.	Угроза несанкционированного доступа к виртуальным каналам передачи	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевое ПО, сетевой трафик, виртуальные устройства
272.	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
273.	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

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
274.	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	виртуальная машина
275.	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
276.	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
277.	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
278.	Угроза ошибки обновления гипервизора	внутренний нарушитель с низким потенциалом	СПО, гипервизор
279.	Угроза перехвата управления гипервизором	внешний нарушитель со средним потенциалом,	СПО, гипервизор, консоль управления гипервизором

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		внутренний нарушитель со средним потенциалом	
280.	Угроза перехвата управления средой виртуализации	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	ИС, СПО
281.	Нарушение доверенной загрузки виртуальных серверов ИС, перехват загрузки*		
282.	Нарушение целостности конфигурации виртуальных серверов - подмена/искажение образов (данных и оперативной памяти) *		
283.	Несанкционированный доступ к консоли управления виртуальной инфраструктурой*		
284.	Несанкционированный доступ к виртуальному серверу ИС, в т.ч. - несанкционированное сетевое подключение и проведение сетевых атак на виртуальный сервер ИС*		
285.	Несанкционированный удаленный доступ к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера»*		
286.	Угроза несанкционированного доступа к объектам виртуальной инфраструктуры без прохождения процедуры идентификации и		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	аутентификации*		
287.	Угроза несанкционированного доступа к виртуальной инфраструктуре/компонентам виртуальной инфраструктуры/виртуальным машинам/объектам внутри виртуальных машин*		
288.	Угроза отсутствия средств регистрации событий в виртуальной инфраструктуре*		
XVI. Угрозы, связанные с нарушением правил эксплуатации машинных носителей			
289.	Угроза несанкционированного восстановления удалённой защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	машинный носитель информации
290.	Угроза несанкционированного удаления защищаемой информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	метаданные, объекты файловой системы, реестр
291.	Угроза утраты носителей информации	внутренний нарушитель с низким потенциалом	носитель информации
292.	Угроза форматирования носителей информации	внешний нарушитель с низким потенциалом, внутренний нарушитель с	носитель информации

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		низким потенциалом	
293.	Повреждение носителя информации		
294.	Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)		
295.	Угроза подключения к ИС неучтенных машинных носителей*		
296.	Угроза подключения к ИС неперсонифицированных машинных носителей		
297.	Угроза несанкционированного копирования информации на машинные носители*		
298.	Угроза несанкционированной модификации/удаления информации на машинных носителях*		
299.	Угроза хищения машинных носителей*		
300.	Угроза подмены машинных носителей*		
301.	Угроза встраивания программно-аппаратных закладок в машинные носители*		
302.	Угроза несанкционированного доступа к информации, хранящейся на машинном носителе*		
303.	Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки		
304.	Угроза использования		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	неконтролируемых портом СВТ для вывода информации на сторонние машинные носители*		
305.	Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей*		
306.	Угроза несанкционированного использования машинных носителей		
307.	Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны		
XVII. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования			
308.	Угроза внедрения вредоносного кода в BIOS	внутренний нарушитель с высоким потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI
309.	Угроза изменения компонентов системы	внутренний нарушитель с низким потенциалом	ИС, сервер, рабочая станция, виртуальная машина, СПО, ППО, аппаратное обеспечение
310.	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	внешний нарушитель со средним потенциалом	микропрограммное обеспечение BIOS/UEFI
311.	Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов*		
312.	Угроза запуска/установки вредоносного/шпионского/нера		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	зрешенного программного обеспечения и(или) обновлений программного обеспечения*		
313.	Установка программного обеспечения, содержащего известные уязвимости*		
314.	Установка нелицензионного программного обеспечения*		
315.	Угроза ошибочного запуска/установки программного обеспечения*		
316.	Угроза неправильной установки программного обеспечения*		
317.	Угроза автоматического запуска вредоносного/шпионского/нера зрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения		
318.	Угроза удаленного запуска/установки вредоносного/шпионского/нера зрешенного программного обеспечения		
319.	Угроза несанкционированного запуска программного обеспечения в нерабочее время		
XVIII. Угрозы физического доступа к компонентам ИС			
320.	Угроза преодоления физической защиты	внешний нарушитель со средним потенциалом	сервер, рабочая станция, носитель информации, аппаратное обеспечение
321.	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
322.	Угроза хищения средств	внешний	сервер, рабочая

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	хранения, обработки и (или) ввода/вывода/передачи информации	нарушитель с низким потенциалом	станция, носитель информации, аппаратное обеспечение
323.	Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ)*		
324.	Угроза нарушение функционирования НЖМД и других систем хранения данных*		
325.	Угроза доступа к системам обеспечения, их повреждение*		
326.	Угроза нарушения функционирования кабельных линий связи, ТС*		
327.	Угроза несанкционированного доступа в контролируемую зону*		
328.	Отсутствие средств автоматизированного контроля доступа		
XIX. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИС, микропрограммном обеспечении			
329.	Угроза анализа криптографических алгоритмов и их реализации	внешний нарушитель со средним потенциалом	метаданные, СПО
330.	Угроза восстановления предыдущей уязвимой версии BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI
331.	Угроза деструктивного использования декларированного функционала BIOS	внутренний нарушитель с низким потенциалом	микропрограммное обеспечение BIOS/UEFI
332.	Угроза использования поддельных цифровых	внешний нарушитель со	микропрограммное и аппаратное

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	подписей BIOS	средним потенциалом	обеспечение BIOS/UEFI
333.	Угроза использования слабых криптографических алгоритмов BIOS	внешний нарушитель с высоким потенциалом	микропрограммное обеспечение BIOS/UEFI
334.	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
335.	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	внешний нарушитель со средним потенциалом	узлы грид-системы
336.	Угроза отключения контрольных датчиков	внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	СПО
337.	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
338.	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

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
339.	Угроза сбоя процесса обновления BIOS	внутренний нарушитель со средним потенциалом	микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи
340.	Угроза установки уязвимых версий обновления программного обеспечения BIOS	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	микропрограммное обеспечение BIOS/UEFI
341.	Угроза перехвата исключения/сигнала из привилегированного блока функций	внешний нарушитель со средним потенциалом, внутренний нарушитель со средним потенциалом	СПО
342.	Угроза наличия механизмов разработчика	внутренний нарушитель со средним потенциалом	ПО, ТС
343.	Угроза «спама» веб-сервера	внешний нарушитель с низким потенциалом	сетевое ПО
XX. Угрозы, связанные с использованием сетевых технологий			
344.	Угроза деавторизации санкционированного клиента беспроводной сети	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	сетевой узел
345.	Угроза заражения DNS-кеша	внешний	сетевой узел,

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		нарушитель с низким потенциалом	сетевое ПО, сетевой трафик
346.	Угроза использования слабостей протоколов сетевого/локального обмена данными	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	СПО, сетевое ПО, сетевой трафик
347.	Угроза неправомерных действий в каналах связи	внешний нарушитель с низким потенциалом	сетевой трафик
348.	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	внешний нарушитель с высоким потенциалом	ИС, аппаратное обеспечение
349.	Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО
350.	Угроза подмены беспроводного клиента или точки доступа	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО, аппаратное обеспечение, точка беспроводного доступа
351.	Угроза подмены доверенного пользователя	внешний нарушитель с низким потенциалом	сетевой узел, сетевое ПО
352.	Угроза подмены субъекта сетевого доступа	внешний нарушитель со средним потенциалом	ППО, сетевое ПО, сетевой трафик
353.	Угроза «фарминга»	внешний	рабочая станция,

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
		нарушитель с низким потенциалом	сетевое ПО, сетевой трафик
354.	Угроза агрегирования данных, передаваемых в грид-системе	внешний нарушитель со средним потенциалом	сетевой трафик
355.	Угроза удаленного запуска приложений		
356.	Угроза навязывания ложных маршрутов*		
357.	Угроза внедрения ложных объектов сети*		
358.	Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа*		
359.	Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений*		
360.	Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений*		
361.	Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений*		
362.	Угроза использования неактуальных версий сигнатур обнаружения атак*		
363.	Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений		
364.	Угроза использования слабостей/уязвимостей защиты		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	протоколов удаленного доступа*		
365.	Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств *		
366.	Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа*		
367.	Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС*		
368.	Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ*		
369.	Угроза подмены сетевых адресов, определяемых по сетевым именам*		
370.	Угроза отсутствия проверки подлинности сетевых соединений*		
371.	Отсутствие подтверждения факта отправки/получения информации конкретными пользователями*		
372.	Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами		
373.	Отсутствие контроля соединений между СВТ ИС		
374.	Угроза несанкционированного доступа к средствам управления		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	информационными потоками		
375.	Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации		
376.	Отсутствие средств анализа сетевого трафика на наличие вредоносного прóграммного обеспечения		
377.	Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны		
XXI. Угрозы инженерной инфраструктуре			
378.	Угрозы сбоев в сети электропитания		
379.	Угроза выхода из строя ТС в результате нарушения климатических параметров работы		
380.	Угрозы нарушения схем электропитания*		
381.	Угрозы связанные с отсутствием заземления/неправильным заземлением *		
XXII. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности			
382.	Угроза отсутствия системы регистрации событий информационной безопасности*		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
383.	Угроза автоматического удаления/затирания событий информационной безопасности новыми события*		
384.	Угроза переполнения журналов информационной безопасности*		
385.	Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ*		
386.	Угроза неправильного отнесения событий, к событиям информационной безопасности*		
387.	Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ*		
388.	Угроза отключения журналов информационной безопасности*		
389.	Угроза модификации/удаления журнала информационной безопасности*		
390.	Угроза задержек при получении журналов информационной безопасности		
391.	Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	времени		
392.	Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности*		
393.	Угроза отключения/отказа системы регистрации событий информационной безопасности		
394.	Угроза несанкционированного изменения правил ведения журнала регистрации событий		
395.	Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности		
XXIII. Угрозы, связанные с контролем защищенности ИС			
396.	Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения *		
397.	Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности*		
398.	Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей		
399.	Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации		
400.	Угроза отсутствия анализа		

№ п/п	Наименование УБ ПДн в ИСПДн	Источники УБ ПДн	Объект воздействия
	изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей*		
401.	Отсутствие журнала анализа защищенности		
XXIV. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи			
402.	Угроза перехвата данных, передаваемых по вычислительной сети	внешний нарушитель с низким потенциалом	сетевой узел, сетевой трафик
403.	Угроза доступа/перехвата/изменения HTTP cookies	внешний нарушитель с низким потенциалом	ППО, сетевое ПО
404.	Угроза перехвата данных *		
405.	Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена		
406.	Угроза перехвата данных с сетевых портов		
407.	Угроза перехвата данных, передаваемых с использованием технологий беспроводного доступа*		

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

* - базовые УБ ПДн в ИСПДн

«ИС» - ИСПДн

«ВЧ» - высокочастотное

«ТС» - технические средства

«БД» - базы данных

«реестр» - стандартный реестр операционной системы

«ВТСС» - вспомогательные технические средства и системы

«СВТ» - средства вычислительной техники

«НСД» - несанкционированный доступ
«НДВ» - недекларированные возможности
«СПО» - системное программное обеспечение
«ППО» - прикладное программное обеспечение
«СЗИ» - средства защиты информации
«СКЗИ» - средства криптографической защиты информации
«ИВК» - измерительно-вычислительный комплекс
«ПЭМИН» - побочные электромагнитные излучения и наводки
«ПО» - программное обеспечение
«ОС» - операционная система
«ПЭВМ» - персональная электронно-вычислительная машина (АРМ)
«НЖМД» - накопитель на жёстких магнитных дисках

Приложение 2
к Угрозам безопасности
персональных
данных, актуальным при обработке
персональных данных в
информационных
системах персональных данных

Типовые возможности нарушителей безопасности информации и направления атак

№ п/п	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия (при наличии)
1	Проведение атаки при нахождении за пределами контролируемой зоны		
2	Проведение атаки при нахождении в пределах контролируемой зоны		
3	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, 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 контролируемой зоны объектов, в которых		

№ п/п	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия (при наличии)
	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	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
8	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО		
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	Проведение работ по созданию способов и		

№ п/п	Возможности нарушителей безопасности информации и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия (при наличии)
	средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		
11	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО		
12	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.		
13	Возможность воздействовать на любые компоненты СКЗИ и СФ		

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

«СКЗИ» - средства криптографической защиты информации

«СФ» - среда функционирования средства криптографической защиты информации

«ПО» - программное обеспечение

«ИС» - информационная система

«СВТ» - средства вычислительной техники