АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «МУНИЦИПАЛЬНЫЙ ОКРУГ ЯРСКИЙ РАЙОН УДМУРТСКОЙ РЕСПУБЛИКИ»

«УДМУРТ ЭЛЬКУНЫСЬ ЯР ЁРОС МУНИЦИПАЛ ОКРУГ» МУНИЦИПАЛ КЫЛДЫТЭТЛЭН АДМИНИСТРАЦИЕЗ

ПОСТАНОВЛЕНИЕ

«30» февраля 2025 года № 425

пос. Яр

Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республике»

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Удмуртской Республики от 6 апреля 2018 года № 103 «Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в исполнительных органах государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и подведомственных им организациях» с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики», Администрация муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» **ПОСТАНОВЛЯЕТ**:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» (далее - Перечень угроз).

2. Отделу организационно-информатизационной работы Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» опубликовать настоящее постановление на официальном сайте

муниципального образования «Муниципальный округ Ярский район Удмуртской Республики».

3. Контроль за исполнением настоящего постановления возложить на Руководителя Аппарата Главы Ярского района, Ярского районного Совета депутатов и Администрации Ярского района Н.В. Леонтьеву.

Глава муниципального образования
«Муниципальный округ Ярский район
Удмуртской Республики» А.Ю. Старцев

УТВЕРЖДЕН
постановлением Администрации
муниципального образования
«Муниципальный округ Ярский район
Удмуртской Республики»
от «4» апреля 2025 года № 425

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики»

I. Общие положения

1. Настоящий Перечень определяет угрозы безопасности персональных данных (далее - УБ ПДн), актуальные при обработке персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн), эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» (далее - Администрация) при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки (далее - Перечень УБ ПДн).

2. В настоящем Перечне УБ ПДн не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

3. Перечень УБ ПДн предназначен для Администрации при решении следующих задач:

1) определение УБ ПДн, актуальных при обработке ПДн в ИСПДн;

2) проведение анализа защищенности ИСПДн от УБ ПДн, актуальных при обработке ПДн в ИСПДн, в ходе выполнения мероприятий по информационной безопасности (защите информации);

3) осуществление модернизации системы защиты ПДн;

4) проведение мероприятий по минимизации и (или) нейтрализации УБ ПДн;

5) предотвращение несанкционированного воздействия на технические средства ИСПДн;

6) осуществление контроля за обеспечением уровня защищенности ПДн.

4. При определении УБ ПДн, актуальных при обработке ПДн в информационных системах персональных данных, эксплуатируемых в Администрации (далее - актуальная УБ ПДн), и совокупности предположений о возможностях нарушителя, которые могут использоваться при создании, подготовке и проведении атак, Администрация с учетом категории ИСПДн, условий и особенностей функционирования ИСПДн, характера и способов обработки ПДн в ИСПДн применяет:

1) группы актуальных УБ ПДн в информационных системах персональных данных, эксплуатируемых в Адмнистрации, приведенные в приложении 1 к настоящему Перечню УБ ПДн;

2) типовые возможности нарушителей безопасности информации и направления атак, приведенные в приложении 2 к настоящему Перечню УБ ПДн.

5. Определение требований к системе защиты информации ИСПДн и выбор средств защиты информации для системы защиты персональных данных с учетом УБ ПДн, определенных в качестве актуальных при обработке ПДн в ИСПДн, осуществляется оператором в соответствии с нормативными правовыми актами, принятыми федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в соответствии с законодательством.

6. В настоящем Перечне УБ ПДн дано описание:

1) категорий ИСПДн как объектов защиты;

2) объектов, защищаемых при определении УБ ПДн в ИСПДн;

3) возможных источников УБ ПДн, обрабатываемых в ИСПДн;

4) возможных видов неправомерных действий и деструктивных воздействий на ПДн в ИСПДн;

5) основных способов реализации УБ ПДн.

7. Список используемых сокращений:

ЕЗСПД - Единая защищенная сеть передачи данных государственных органов Удмуртской Республики, функционирующая в соответствии с постановлением Правительства Удмуртской Республики от 16 апреля 2012 года № 169 «Об утверждении Положения о Единой защищенной сети передачи данных государственных органов Удмуртской Республики». Подключение к данной сети ее участников осуществляется с применением сертифицированных аппаратно-программных комплексов шифрования "VipNetCoordinator";

ЗСПД - защищенные сети персональных данных исполнительных органов государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и подведомственных им организациях, органов местного самоуправления, функционирующих для обеспечения их деятельности на территории Удмуртской Республики. Подключение к данным сетям их участников осуществляется с применением сертифицированных аппаратно-программных комплексов шифрования "VipNetCoordinator" и программных комплексов шифрования "VipNetClient";

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;

ВЧ - высокочастотный;

ТС - технические средства;

ВТСС - вспомогательные технические средства;

ИВК - информационно-вычислительный комплекс;

ИС - информационная система;

ПЭМИН - побочное электромагнитное излучение;

ПАК - программно-аппаратный комплекс;

КЗ - контролируемая зона.

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

8. Владельцами ИСПДн и их операторами являются федеральные государственные органы, исполнительные органы государственной власти Удмуртской Республики, подведомственные им организации, Администрация муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» и иные организации.

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

10. Контролируемой зоной ИСПДн, функционирующих в Администрации, являются здания и отдельные помещения, принадлежащие ей или находящиеся в ее владении и (или) пользовании на законных основаниях. Все СВТ, участвующие в обработке ПДн, располагаются в пределах контролируемой зоны Администрации. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование оператора связи (провайдера), используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена и расположенное за пределами территории Администрации.

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

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

2) сетям государственных органов и организаций, расположенных на территории Российской Федерации. Подключение к данным сетям осуществляется в соответствии с регламентами взаимодействия. Администрация имеет подключение к ЕЗСПД и ЗСПД посредством защищенных каналов связи.

12. Подключение к сетям связи общего пользования осуществляется Администрацией при условии соблюдения ими мер по обеспечению безопасности передаваемых персональных данных, в том числе мер по защите информационных систем персональных данных, средств и систем связи и передачи данных.

III. Объекты защиты и технологии обработки персональных данных в информационных системах персональных данных

13. При определении Администрацией УБ ПДн в конкретной ИСПДн в обязательном порядке защите подлежат следующие объекты, входящие в ИСПДн:

1) персональные данные, обрабатываемые в информационных системах персональных данных;

2) информационные ресурсы информационных систем персональных данных (файлы, базы данных и т.п.);

3) средства вычислительной техники, участвующие в обработке персональных данных посредством информационных систем персональных данных;

4) аппаратное обеспечение средств вычислительной техники, участвующих в обработке персональных данных посредством информационных систем персональных данных;

5) программное (микропрограммное, системное и прикладное) обеспечение СВТ, участвующих в обработке персональных данных посредством информационных систем персональных данных;

6) средства криптографической защиты информации;

7) среда функционирования СКЗИ;

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

9) 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;

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

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

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

13) сетевой трафик;

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

15) помещения, в которых находятся ресурсы ИСПДн, имеющие отношение к криптографической защите ПДн;

16) системы обеспечения ИСПДн.

14. В состав средств вычислительной техники, участвующих в обработке персональных данных посредством информационных систем персональных данных, входят:

1) автоматизированные рабочие места пользователей с различными уровнями доступа (правами) (далее также - АРМ), представляющие собой программно-аппаратные комплексы, позволяющие осуществлять доступ пользователей к информационным системам персональных данных и предназначенные для локальной обработки информации;

2) серверное оборудование, представляющее собой программно-аппаратный комплекс в совокупности с программным и информационным обеспечением для его управления (общесистемное программное обеспечение (операционные системы физических серверов, виртуальных серверов, АРМ и т.п.), прикладное программное обеспечение (системы управления базами данных и т.п.), предназначенный для обработки и консолидированного хранения персональных данных информационных систем персональных данных. Серверное оборудование может быть представлено автоматизированными рабочими местами пользователей с различными уровнями доступа (правами), выполняющими функции сервера;

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

15. Ввод персональных данных в информационные системы персональных данных осуществляется как с бумажных носителей, так и с электронных носителей

информации. Персональные данные выводятся из информационных систем персональных данных как в электронном, так и в бумажном виде с целью их использования, хранения и (или) передачи третьим лицам.

IV. Общее описание информационных систем персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики» при осуществлении соответствующих видов деятельности

16. С целью исполнения своих полномочий (функций) в Администрации обрабатываются все категории ПДн. Состав ПДн, подлежащих обработке в конкретной ИСПДн, цели обработки, действия (операции), совершаемые с ПДн в ИСПДн, определяются Администрацией, являющейся оператором ИСПДн. Обработка ПДн в ИСПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных». Перечень обрабатываемых ПДн в ИСПДн должен соответствовать целям их обработки. ИСПДн и ее компоненты должны быть расположены в пределах Российской Федерации.

ИСПД подразделяются на:

1) ИСПДн, оператором которым является сама Администрация;

2) ИСПДн, эксплуатируемые Администрацией, но не в качестве ее оператора.

Для всех категорий персональных данных, обрабатываемых в информационных системах персональных данных, за исключением общедоступных персональных данных, требуется обеспечить следующие характеристики безопасности: конфиденциальность, целостность, доступность и подлинность информации. При обработке общедоступных персональных данных требуется обеспечить следующие характеристики безопасности: целостность, доступность и подлинность информации.

17. Информационные системы персональных данных, эксплуатируемые в Администрации при осуществлении соответствующих видов деятельности, в зависимости от технологии обработки персональных данных, состава персональных данных и целей их обработки подразделяются на:

1) информационно-справочные;

2) сегментные;

3) региональные;

4) служебные.

V. Информационно-справочные системы персональных данных

18. Информационно-справочные ИСПДн используются для официального доведения любой информации до определенного или неопределенного круга лиц, при этом факт доведения такой информации не порождает правовых последствий, однако может являться обязательным в соответствии с законодательством.

19. К информационно-справочным ИСПДн относится официальный сайт муниципального образования «Муниципальный округ Ярский район Удмуртской Республики».

20. Официальный сайт муниципального образования «Муниципальный округ Ярский район Удмуртской Республики».

ИСПДн содержат сведения о деятельности органов местного самоуправления, в том числе сведения, подлежащие обязательному опубликованию в соответствии с законодательством.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

1) общедоступные;

2) иные.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн может осуществляться посредством веб-интерфейса сотрудниками Администрации и иными физическими лицами. ПДн хранятся в базе данных ИСПДн и отображаются по запросу соответствующей страницы ИСПДн пользователям в соответствии с предоставленными правами.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся сотрудники Администрации и иные физические лица.

ИСПДн по структуре является функционирующей на серверном оборудовании государственных органов и организаций в пределах их контролируемых зон, и (или) на вычислительных ресурсах облачного провайдера.

ИСПДн подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн относится к подключенном с использованием иных каналов связи.

Средства вычислительной техники, используемые для обработки персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

VI. Сегментные информационные системы персональных данных

21. Сегментные ИСПДн представляют собой сегменты федеральных информационных систем, которые создаются и эксплуатируются на уровне Удмуртской Республики на основании предоставляемых с федерального уровня рекомендаций (правовых, организационных, технических), и используются для сбора, обработки, свода данных на уровне Удмуртской Республики и передачи их на федеральный уровень, и наоборот, при этом цели и задачи создания (модернизации), эксплуатации данных информационных систем определяются на федеральном уровне. Сегментные ИСПДн предназначены для реализации полномочий федеральных органов власти и исполнения функций Администрации.

Обработке в ИСПДн могут подлежать все категории ПДн.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками Администрации в специализированных программах и (или) посредством веб-интерфейса, и в отдельных случаях физическими лицами в режиме веб-интерфейса (с ограниченными правами доступа).

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся физические лица.

Структура ИСПДн является распределенной или локальной, функционирующей в контролируемой зоне Администрации.

ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

1) подключенные посредством ЕЗСПД и ЗСПД;

2) подключенные с использованием иных каналов связи.

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

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

2) подключенные посредством ЕЗСПД и ЗСПД;

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

Средства вычислительной техники, используемые для обработки персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

1) построенные по технологии «толстого клиента» (на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту, располагающемуся в пределах контролируемой зоны Администрации, и передающее данные на центральный сегмент или напрямую на центральный сервер, либо 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 с нарочным);

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

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

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

2) реализованные с использованием терминального доступа с авторизацией с помощью логина и пароля и (или) электронного сертификата, и (или) сертификата ключа проверки электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи».

VII. Региональные информационные системы персональных данных

22. Региональные ИСПДн создаются и эксплуатируются по решению исполнительных органов государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и подведомственных им организаций в интересах государственных органов Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики, при этом цели и задачи создания (модернизации), эксплуатации региональных ИСПДн, а также требования к ним определяются в решениях исполнительных органов государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и подведомственных им организаций.

По выполняемым функциям ИСПДн подразделяются на:

1) многопрофильные (например, Система межведомственного электронного документооборота государственных органов Удмуртской Республики, Система исполнения регламентов Удмуртской Республики);

2) ИСПДн для исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики.

23. ИСПДн многопрофильные.

Многопрофильные ИСПДн предназначены для централизованной автоматизации делопроизводства и документооборота, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам и т.п. в исполнительных органах государственной власти Удмуртской Республики, иных государственных (муниципальных) органах и (или) организациях на территории Удмуртской Республики.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

1) специальные;

2) иные;

3) общедоступные.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется сотрудниками в специализированных программах в соответствии с предоставленными правами.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся физические лица.

Структура ИСПДн является локальной или распределенной, функционирующей в контролируемой зоне).

ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

1) подключенные посредством ЕЗСПД и ЗСПД;

2) подключенные с использованием иных каналов связи.

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

1) посредством ЕЗСПД и ЗСПД;

2) с использованием сторонних СКЗИ.

Средства вычислительной техники, участвующие в обработке персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

24. ИСПДн для исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики.

ИСПДн предназначены для автоматизации совместной деятельности исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики, в том числе деятельности, осуществление которой необходимо в соответствии с законодательством.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

1) общедоступные;

2) иные.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется в соответствии с предоставленными правами сотрудниками в специализированных программах в режиме веб-интерфейса.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся сотрудники исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики.

Структура ИСПДн является локальной, функционирующей в контролируемой зоне исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики.

ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

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

2) подключенные посредством ЕЗСПД и ЗСПД;

3) подключенные с использованием иных каналов связи.

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

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

2) посредством ЕЗСПД и ЗСПД;

3) с использованием сторонних СКЗИ.

Средства вычислительной техники, участвующие в обработке персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

25. По архитектуре региональные ИСПДн подразделяются на:

1) сегментированные;

2) централизованные;

3) смешанные.

26. Сегментированные ИСПДн делятся на центральный и периферийный сегменты, 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, выполняющие функции сервера, или серверное оборудование. Пользователи периферийных сегментов подключаются к расположенным в пределах контролируемой зоны АРМ, выполняющим функции сервера, или серверному оборудованию, осуществляющему консолидацию сведений на уровне периферийного сегмента, который, в свою очередь, передает полученные данные в центральный сегмент.

27. По технологии обработки ИСПДн подразделяются на:

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

2) построенные по технологии «тонкого клиента» (на рабочие места пользователей ИСПДн передается только графическая информация, при этом сама обработка данных осуществляется на серверном сегменте, располагающемся в пределах контролируемой зоны и передающем данные на центральный сегмент).

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

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

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

28. Централизованные ИСПДн делятся на центральный и периферийный сегменты.

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.

29. По технологии обработки ИСПДн подразделяются на:

1) построенные по технологии «толстого клиента» (на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к центральному сегменту, или 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 с нарочным);

2) построенные по технологии «тонкого клиента» (на рабочие места пользователей ИСПДн передается только графическая информация, при этом сама обработка данных осуществляется на центральном сегменте).

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

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

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

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

VIII. Служебные информационные системы персональных данных

31. Служебные ИСПДн создаются (эксплуатируются) по решению Администрации, цели и задачи создания (модернизации), эксплуатации которых определяются Администрацией, и используются для автоматизации определенной области деятельности или типовой деятельности, неспецифичной относительно полномочий Администрации. Служебные ИСПДн предназначены для управления бизнес-процессами в Администрации.

32. К основным служебным ИСПДн относятся, например:

1) ИСПДн бухгалтерского учета, управления финансами, пенсионного фонда и налоговых служб;

2) ИСПДн кадрового учета и управления персоналом;

3) ИСПДн поддерживающие.

33. ИСПДн бухгалтерского учета, управления финансами, пенсионного фонда и налоговых служб.

ИСПДн предназначены для автоматизации деятельности Администрации, связанной с ведением бухгалтерского учета, управлением финансами, осуществлением пенсионных отчислений и уплатой налогов.

Обработке в ИСПДн подлежат категории ПДн, указанные в абзаце четвертом пункта 5 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1118.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации и(или) обслуживающей организации в

специализированных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся сотрудники Администрации, являющегося оператором ИСПДн.

Структура ИСПДн является локальной, функционирующей в контролируемой зоне Администрации. ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

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

2) подключенные посредством ЕЗСПД и ЗСПД;

3) подключенные с использованием иных каналов связи.

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

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

2) с использованием сторонних СКЗИ.

Средства вычислительной техники, участвующие в обработке персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

1) построенные по технологии «толстого клиента» (на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая размещается на серверном сегменте (сервере/автоматизированном рабочем месте, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Администрации;

2) построенные по технологии «тонкого клиента» (на рабочие места пользователей ИСПДн передается только графическая информация, при этом сама обработка данных осуществляется на удаленном серверном сегменте (сервере/автоматизированном рабочем месте, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Администрации.

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

34. ИСПДн кадрового учета и управления персоналом.

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

Категории ПДн, которые могут подлежать обработке в ИСПДн:

1) специальные;

2) иные.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных и (или) стандартных офисных программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся сотрудники Администрации, являющегося оператором ИСПДн, и физические лица, имеющие трудовые отношения с Администрацией и (или) претендующими на замещение должностей в Администрации.

Структура ИСПДн является локальной, функционирующей в контролируемой зоне Администрации.

ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

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

2) подключенные посредством ЕЗСПД и ЗСПД;

3) подключенные с использованием иных каналов связи.

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

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

2) с использованием сторонних СКЗИ.

Средства вычислительной техники, участвующие в обработке персональных данных:

1) автоматизированные рабочие места;

2) сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

1) построенные по технологии «толстого клиента» (на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к базе данных, которая размещается на серверном сегменте (сервере/автоматизированном рабочем месте, выполняющем функцию сервера), располагающемся в пределах контролируемой зоны Администрации. Доступ к ПДн в ИСПДн предоставляется пользователю после ввода логина и пароля (предъявления идентификатора);

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

3) построенные по веб-технологии (пользователи осуществляют деятельность в ИСПДн посредством веб-интерфейса).

35. ИСПДн поддерживающие.

ИСПДн предназначены для автоматизации деятельности Органов и Организаций, связанной с осуществлением ими (их сотрудниками) своих функций, полномочий и задач.

Категории ПДн, которые могут подлежать обработке в ИСПДн:

1) специальные;

2) иные;

3) общедоступные.

Режим обработки ПДн в ИСПДн является многопользовательским. ИСПДн предусматривают разграничение доступа. Обработка ПДн осуществляется сотрудниками Администрации в специализированных и (или) стандартных офисных

программах и (или) посредством веб-интерфейса в соответствии с предоставленными правами.

К субъектам, персональные данные которых могут подлежать обработке в ИСПДн, относятся сотрудники Администрации, являющегося оператором ИСПДн, и иные физические лица.

Структура ИСПДн является локальной, функционирующей в контролируемой зоне Администрации.

ИСПДн подключены к сетям связи общего пользования и (или) сетям международного информационного обмена.

По типу подключения ИСПДн делятся на:

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

2) подключенные посредством ЕЗСПД и ЗСПД;

3) подключенные с использованием иных каналов связи.

Передача ПДн в иные ИСПДн не осуществляется.

Средства вычислительной техники, участвующие в обработке персональных данных:

1) автоматизированные рабочие места;

2) серверное оборудование;

3) сетевое и телекоммуникационное оборудование.

По технологии обработки ИСПДн подразделяются на:

1) построенные по принципу «толстого клиента» (на рабочие места пользователей ИСПДн устанавливается специальное клиентское приложение, осуществляющее подключение к серверному сегменту (серверу/автоматизированному рабочему месту, выполняющему функцию сервера), располагающемуся в пределах контролируемой зоны Администрации;

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

3) построенные по веб-технологии (пользователи осуществляют деятельность в ИСПДн посредством веб-интерфейса, подключающегося к локальному веб-серверу, располагающемуся в пределах контролируемой зоны Администрации.

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

IX. Угрозы безопасности персональных данных, выявленные при функционировании информационных систем персональных данных

36. Источники УБ ПДн в ИСПДн.

Источниками УБ ПДн в ИСПДн выступают:

1) носитель вредоносной программы;

2) аппаратная закладка;

3) нарушитель.

37. 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:

1) отчуждаемый носитель (дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый жесткий диск и т.п.);

2) встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессоры, 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);

3) 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:

1) пакеты передаваемых по компьютерной сети сообщений;

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

38. Аппаратная закладка.

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

1) аппаратная закладка внутри клавиатуры;

2) аппаратная закладка для считывания данных с кабеля клавиатуры бесконтактным методом;

3) аппаратная закладка в виде устройства, включенного в разрыв кабеля;

4) аппаратная закладка внутри системного блока.

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

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

39. Нарушитель.

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

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

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

2) внутренний нарушитель, имеющий доступ к ИСПДн. Данный тип нарушителя имеет право постоянного или периодического доступа на территорию КЗ, а также доступ к техническим средствам и ресурсам ИСПДн, расположенным в пределах КЗ. Внутренний нарушитель, имеющий доступ к ИСПДн, может проводить

атаки с использованием внутренней (локальной) сети передачи данных и непосредственно в ИСПДн;

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

40. Основные УБ ПДн в ИСПДн:

1) угрозы утечки информации по техническим каналам;

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

3) угрозы нарушения доступности информации;

4) угрозы нарушения целостности информации;

5) угрозы НДВ в СПО и ППО;

6) угрозы, не являющиеся атаками;

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

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

9) угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн;

10) угрозы ошибочных/деструктивных действий лиц;

11) угрозы нарушения конфиденциальности;

12) угрозы программно-математических воздействий;

13) угрозы, связанные с использованием облачных услуг;

14) угрозы, связанные с использованием технологий виртуализации;

15) угрозы, связанные с нарушением правил эксплуатации машинных носителей;

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

17) угрозы физического доступа к компонентам ИСПДн;

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

19) угрозы, связанные с использованием сетевых технологий;

20) угрозы инженерной инфраструктуры;

21) угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

22) угрозы, связанные с контролем защищенности ИСПДн;

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

X. Меры, направленные на минимизацию угроз безопасности персональных данных в информационных системах персональных данных

41. При обработке ПДн в ИСПДн Администрации применяют правовые, организационные и технические меры, установленные законодательством, а также руководствуются следующими документами:

приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

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

приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 года;

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

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

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

Методическими рекомендациями по разработке нормативных правовых актов, определяющими угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432;

Банком данных угроз безопасности, сформированным Федеральной службой по техническому и экспортному контролю и Государственным научно-исследовательским испытательным институтом проблем технической защиты информации.

42. Реализация правовых, организационных и технических мер, направленных на минимизацию УБ ПДн в ИСПДн, осуществляется специалистами по

информационной безопасности (технической защите информации) Администрации, ответственными за планирование, организацию и реализацию мероприятий по обеспечению информационной безопасности в Администрации.

Приложение 1
к Перечню
угроз безопасности персональных
данных, актуальных при обработке
персональных данных в информационных
системах персональных данных,
эксплуатируемых в Администрации
муниципального образования
«Муниципальный округ Ярский район
Удмуртской Республики»

Актуальные угрозы безопасности персональных данных
в информационных системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики»

№ п/п	Наименование информационных систем персональных данных	Актуальные угрозы безопасности персональных данных
1	Информационно-справочные информационные системы персональных данных	
1.1	Официальный сайт муниципального образования «Муниципальный округ Ярский район Удмуртской Республики»	угрозы использования штатных средств с целью совершения несанкционированного доступа (далее - НСД) к информации; угрозы нарушения доступности информации; угрозы нарушения целостности информации; угрозы недекларированных возможностей (далее - НДВ) в системном программном обеспечении (далее также - СПО) и прикладном программном обеспечении (далее - ППО); угрозы, не являющиеся атаками; угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации; угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;

		угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн; угрозы ошибочных/деструктивных действий лиц; угрозы нарушения конфиденциальности; угрозы программно-математических воздействий; угрозы, связанные с использованием облачных услуг <*>; угрозы, связанные с использованием технологий виртуализации <**>; угрозы, связанные с нарушением правил эксплуатации машинных носителей; угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования; угрозы эксплуатации уязвимостей в СПО, ППО, средствах защиты информации (далее также - СЗИ), средствах криптографической защиты информации (далее также - 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	Сегментные информационные системы персональных данных	угрозы использования штатных средств ИСПДн с целью совершения НСД к информации; угрозы нарушения доступности информации; угрозы нарушения целостности информации; угрозы НДВ в СПО и ППО; угрозы, не являющиеся атаками;

		угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации; угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом; угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн; угрозы ошибочных/деструктивных действий лиц; угрозы нарушения конфиденциальности; угрозы программно-математических воздействий; угрозы, связанные с использованием облачных услуг <*>; угрозы, связанные с использованием технологий виртуализации <**>; угрозы, связанные с нарушением правил эксплуатации машинных носителей; угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования; угрозы 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	Региональные информационные системы персональных данных	
3.1	Интеграционные	угрозы утечки информации по

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

		угрозы инженерной инфраструктуры; угрозы, связанные с отсутствием системы регистрации событий информационной безопасности; угрозы, связанные с контролем защищенности ИСПДн; угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи
3.2	Многопрофильные информационные системы персональных данных	угрозы утечки информации по техническим каналам; угрозы использования штатных средств ИСПДн с целью совершения НСД к информации; угрозы нарушения доступности информации; угрозы нарушения целостности информации; угрозы НДВ в СПО и ППО; угрозы, не являющиеся атаками; угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации; угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом; угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн; угрозы ошибочных/деструктивных действий лиц; угрозы нарушения конфиденциальности; угрозы программно-математических воздействий; угрозы, связанные с использованием облачных услуг <*>; угрозы, связанные с использованием технологий виртуализации <**>; угрозы, связанные с нарушением правил эксплуатации машинных носителей; угрозы, связанные с нарушением процедур установки/обновления программного

		обеспечения и оборудования; угрозы физического доступа к компонентам ИСПДн; угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении; угрозы, связанные с использованием сетевых технологий; угрозы инженерной инфраструктуры; угрозы, связанные с отсутствием системы регистрации событий информационной безопасности; угрозы, связанные с контролем защищенности ИСПДн; угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи
3.3	Информационные системы персональных данных для исполнительных органов государственных власти Удмуртской Республики, иных государственных (муниципальных) органов и (или) организаций на территории Удмуртской Республики	угрозы утечки информации по техническим каналам; угрозы использования штатных средств ИСПДн с целью совершения НСД к информации; угрозы нарушения доступности информации; угрозы нарушения целостности информации; угрозы НДВ в СПО и ППО; угрозы, не являющиеся атаками; угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации; угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом; угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы информационной безопасности ИСПДн; угрозы ошибочных/деструктивных действий лиц; угрозы нарушения конфиденциальности; угрозы программно-математических воздействий;

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

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

Примечание:
* Актуальны при использовании в информационной системе облачных услуг;
** Актуальны при использовании в информационной системе.

Приложение 2
к Перечню
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных
системах персональных данных, эксплуатируемых в Администрации муниципального образования «Муниципальный округ Ярский район Удмуртской Республики»

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 средств криптографической защиты информации (далее - СКЗИ) на документацию на СКЗИ и компоненты среды функционирования (далее также - СФ) и помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СПТ), на которых реализованы СКЗИ и СФ		
4	Получение в рамках предоставленных полномочий, а также в результате наблюдений сведений о физических мерах защиты объектов, в которых размещены ресурсы		

	информационной системы, сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы, и сведений о мерах по разграничению доступа в помещения, в которых находятся СПТ, на которых реализованы СКЗИ и СФ		
5	Использование штатных средств информационных систем персональных данных (далее - ИСПДн), ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
6	Физический доступ к СПТ, на которых реализованы СКЗИ и СФ		
7	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
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 программного обеспечения (далее - ПО)		
9	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение		

	несанкционированных действий		
10	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		
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 определяются в частных моделях угроз и нарушителя безопасности информации для каждой информационной системы персональных данных.