АДМИНИСТРАЦИЯ
ЕРШОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
САРАТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 21.07.2021 № 460

г.Ершов

О внесении изменений в Постановление администрации Ершовского муниципального района Саратовской области от 15.07.14 № 931

В соответствии с требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Устава Ершовского муниципального района Саратовской области и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, администрация Ершовского муниципального района ПОСТАНОВЛЯЕТ:

1. Внести в постановление администрации Ершовского муниципального района Саратовской области от 15.07.14 № 931 "Об утверждении документов, определяющих политику в отношении обработки персональных данных в администрации Ершовского муниципального района Саратовской области" следующие изменения:

1.1. Название постановления изложить в следующей редакции: "Политика администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных";

1.2. Пункт 1.1 "Документ, аккумулирующий информацию о персональных данных (Приложение №1)" изложить в новой редакции: "Модель угроз информационной системы персональных данных администрации Ершовского муниципального района Саратовской области (ИСПДн Администрации ЕМР)" согласно Приложению №1 к настоящему постановлению;

1.3. Пункт 1.2 "Перечень персональных данных, обрабатываемых в администрации Ершовского муниципального района Саратовской области." (Приложение №2) изложить в новой редакции согласно Приложению №2 к настоящему постановлению;

1.4. Пункт 1.3 "Перечень лиц, должностей допущенных к обработке персональных данных." (Приложение №3) изложить в новой редакции согласно Приложению №3 к настоящему постановлению;

1.5. Пункт 1.4 " Перечень информационных систем по обработке персональных данных" (Приложение №4) изложить в новой редакции согласно Приложению №4 к настоящему постановлению;

1.6. Пункт 1.5 "Положение о персональных данных и их защите (Приложение №5)" изложить в новой редакции: "Политика администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных" согласно Приложению №5 к настоящему постановлению;

1.7. Пункт 1.6 "Должностная инструкция сотрудников, имеющих отношение к обработке персональных данных (Приложение №6)" изложить в новой редакции: "Правила работы с персональными данными для сотрудников администрации Ершовского муниципального района Саратовской области, в обязанности которых входит регистрация, рассмотрение запросов субъектов персональных данных, обработка и защита персональных данных." согласно Приложению №6 к настоящему постановлению;

1.8. Пункт 1.7 "Порядок доступа служащих администрации Ершовского муниципального района в помещения, в которых ведется обработка персональных данных (Приложение №7)" изложить в новой редакции: "Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения" согласно Приложению №7 к настоящему постановлению;

2. Отделу по информатизации и программному обеспечению администрации Ершовского муниципального района разместить настоящее постановление на официальном сайте администрации района в информационно-телекоммуникационной сети «Интернет» (https://adminemr.ru);

3.Контроль за исполнением данного постановления возложить на руководителя аппарата администрации Ершовского муниципального района Калинину С.В.

Глава Ершовского муниципального района С.А. Зубрицкая

Приложение №1 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

МОДЕЛЬ УГРОЗ
информационной системы персональных данных Администрации.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ..... (3)
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ..... (4)
1 ВВЕДЕНИЕ..... (8)
2 НАЗНАЧЕНИЕ, СТРУКТУРА И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИСПД ТБ..... (9)
3 МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ...(12)
3.1 ОПИСАНИЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ..... (12)
3.2 ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩЕЙСЯ У НАРУШИТЕЛЯ ИНФОРМАЦИИ ОБ ОБЪЕКТАХ РЕАЛИЗАЦИИ УГРОЗ..... (14)
3.3 ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩИХСЯ У НАРУШИТЕЛЯ СРЕДСТВАХ РЕАЛИЗАЦИИ ГРОЗ..... (15)
3.4 ОПИСАНИЕ ОБЪЕКТОВ И ЦЕЛЕЙ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... (15)
3.5 ОПИСАНИЕ КАНАЛОВ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... (16) 3.6 ОСНОВНЫЕ СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... (16)
4. ИСХОДНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИСПДн..... (17)
5. ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ..... (17)

5.1. УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ.....
18)
5.1.1. УГРОЗЫ УТЕЧКИ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ.....
(18)
5.1.2. УГРОЗЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ.....
(18)
5.1.3.УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИН.....
(18)
5.2.УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ.....(18)
5.2.1.УГРОЗЫ УНИЧТОЖЕНИЯ, ХИЩЕНИЯ АППАРАТНЫХ СРЕДСТВ ИСПДн НОСИТЕЛЕЙ ИНФОРМАЦИИ ПУТЕМ ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИСПДн.....
(18)
5.2.2. УГРОЗЫ ХИЩЕНИЯ, НЕСАНКЦИОНИРОВАННОЙ МОДИФИКАЦИИ ИЛИ БЛОКИРОВАНИЯ ИНФОРМАЦИИ ЗА СЧЕТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД) С ПРИМЕНЕНИЕМ ПРОГРАММНО-АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ (В ТОМ ЧИСЛЕ ПРОГРАММНО-МАТЕМАТИЧЕСКИХ ВОЗДЕЙСТВИЙ).....(20)
5.2.3 .УГРОЗЫ НЕ ПРЕДНАМЕРЕННЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ И НАРУШЕНИЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ИСПДН И СЗПДН В ЕЕ СОСТАВЕ ИЗ-ЗА СБОЕВ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, А ТАКЖЕ ОТ УГРОЗ НЕАНТРОПОГЕННОГО (СБОЕВ АППАРАТУРЫ ИЗ-ЗА НЕНАДЕЖНОСТИ ЭЛЕМЕНТОВ, СБОЕВ ЭЛЕКТРОПИТАНИЯ) И СТИХИЙНОГО (УДАРОВ МОЛНИЙ, ПОЖАРОВ, НАВОДНЕНИЙ И Т.П.) ХАРАКТЕРА.....(20)
5.2.4. УГРОЗЫ ПРЕДНАМЕРЕННЫХ ДЕЙСТВИЙ ВНУТРЕННИХ НАРУШИТЕЛЕЙ.....(22)
5.2.5. УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПО КАНАЛАМ СВЯЗИ.....(22)
6. РЕАЛИЗУЕМОСТЬ УГРОЗ.....
(26)
7. ОЦЕНКА ОПАСНОСТИ УГРОЗ.....
(28)
8. ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ В ИСПДн.....
(30)
9. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ.....
(32)
10. ЗАКЛЮЧЕНИЕ.....
(37)

Сокращения

АВС – антивирусные средства
АС – автоматизированная система
АРМ – автоматизированное рабочее место
БД – база данных
ВТСС – вспомогательные технические средства и системы
ИКХ – информация конфиденциального характера
ИСПДн – информационная система персональных данных
ИСПДн ТБ - информационная система персональных данных «Турбо- Бухгалтер»
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
НСД – несанкционированный доступ к информации
МЭ – межсетевой экран
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ППО – прикладное программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СВТ – средства вычислительной техники
СЗИ – средство защиты информации
СЗПДн – система защиты персональных данных
СОВ – система обнаружения вторжений
СФ – среда функционирования
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных
ФСТЭК России – Федеральная служба по техническому и экспортному контролю

Термины и определения

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе

данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение),

использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в

информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1.Введение

Настоящий документ подготовлен в рамках выполнения работ по построению системы защиты персональных данных (далее – СЗПДн), не содержащей сведений, составляющих государственную тайну, информационной системы персональных данных Администрации (далее-ИСПДн).

Настоящий документ содержит модель угроз безопасности персональных данных для ИСПДн (далее – модель угроз).

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации ИСПДн и проектирования ИСПДн.

Модель угроз – документ, использующийся для:

- анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроля обеспечения уровня защищенности персональных данных.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз.
- Оценку вероятности возникновения угроз.
- Оценку реализуемости угроз.
- Оценку опасности угроз.
- Определение актуальности угроз.

Модель угроз для ИСПДн разрабатывается в соответствии со следующими нормативными и методологическими документами:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
- Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

В процессе развития ИСПДн предполагается конкретизировать и пересматривать модель угроз для ИСПДн.

Модель угроз может быть пересмотрена:

по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

При разработке модели угроз для ИСПДн учитывается, что ИСПДн является специальной информационной системой т.к., к обрабатываемым в ней данным предъявляются требования не только по конфиденциальности, но и по целостности и доступности.

2 Назначение, структура и основные характеристики ИСПДн

Информационная система персональных данных Администрации предназначена для поддержки технологических процессов работы отраслевых (функциональных) органов администрация не являющихся юридическими лицами и материального обеспечения Администрации.

Информационная система персональных данных Администрации позволяет:

-Исполнение условий трудового договора (служебного контракта) и осуществление прав и обязанностей в соответствии с трудовым законодательством, законодательством о муниципальной службе;

-Рассмотрение обращений граждан Российской Федерации в соответствии с законодательством;

-Выполнение обязательств по гражданско-правовым договорам (контрактам) и иным соглашениям, заключаемым с Администрацией;

-Предоставление муниципальных услуг, реализация полномочий органа местного самоуправления;

-Создание общедоступных источников персональных данных.

Рассматриваемая ИСПДн имеет подключение к сетям общего пользования и международного обмена.

Все компоненты ИСПДн находятся на одном объекте вычислительной техники внутри контролируемой зоны.

Обработка персональных данных в ИСПДн ведется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Основные параметры ИСПДн приведены в Таблице 1.

Таблица 1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации

Дополнительная информация	К персональным данным предъявляется требование целостности и доступности

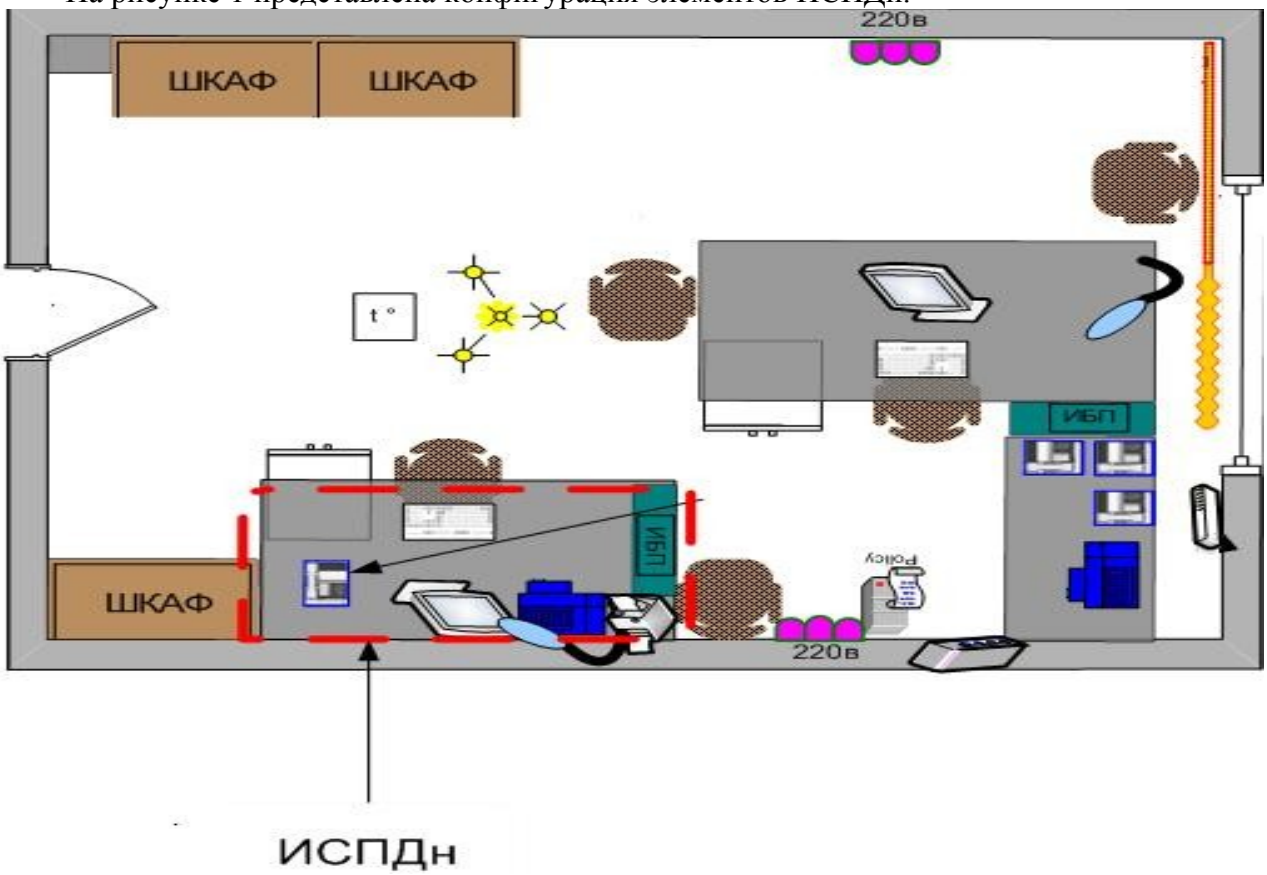
В ИСПД обрабатываются следующие типы ПДн:

-тип ПД, обрабатываемые Оператором перечислены в Приложении №2 к постановлению администрации ЕМР № 931 от 15.07.2014 г.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **ВТОРОЙ категории персональных данных,** т.е. к данным, позволяющим идентифицировать субъекта персональных данных и получить о нем дополнительную информацию.

Объем обрабатываемых персональных данных, **не превышает 1000 записей** о субъектах персональных данных.

На рисунке 1 представлена конфигурация элементов ИСПДн.



На рисунке 2 представлено границы контролируемой зоны.

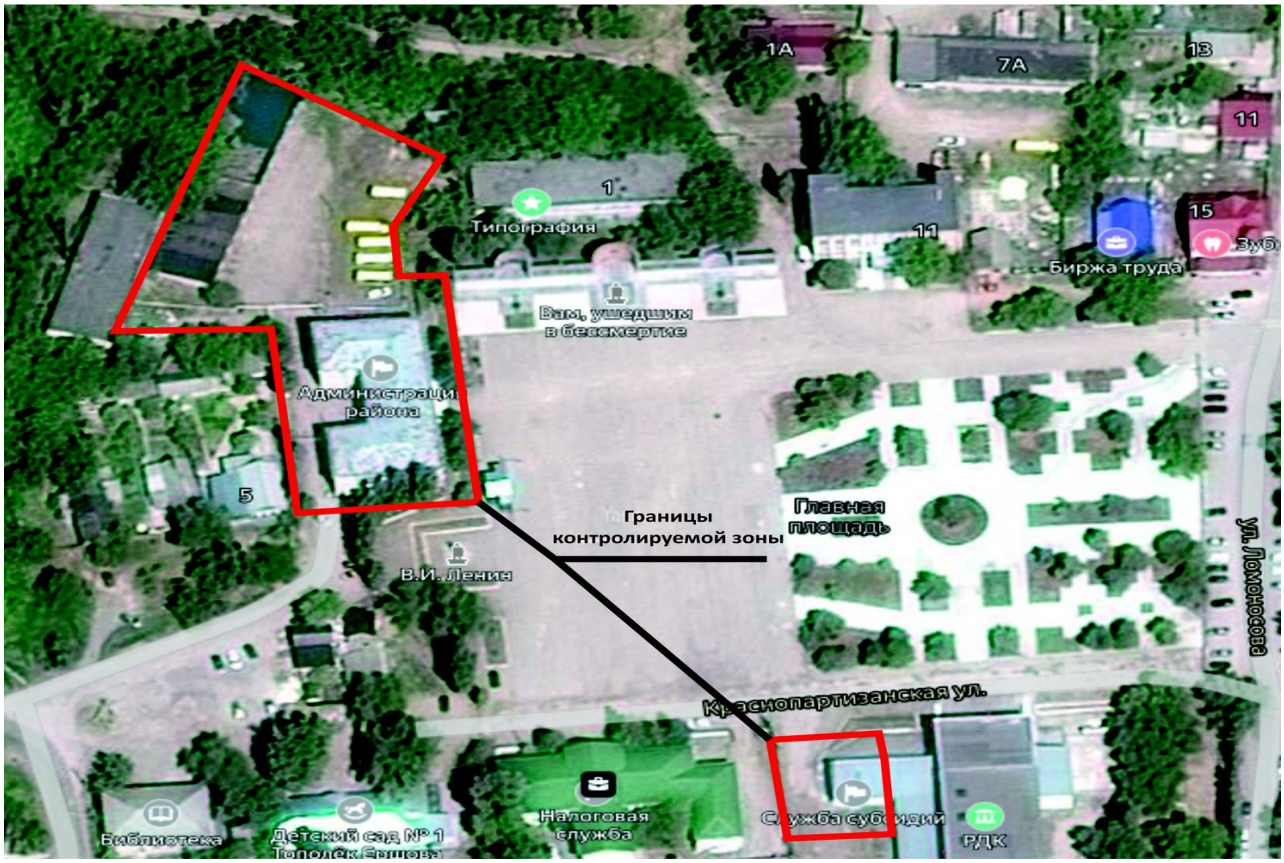


Рисунок 2.

Для функционирования прикладных программ в состав ИСПДн входит следующее специальное оборудование:

- Лазерный принтер, подключенный к разъему USB системного блока;
- Сканер, подключенный к разъему USB системного блока.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. ИСПДн располагает необходимыми данными для идентификации, аутентификации, а также препятствует несанкционированному доступу к ресурсам.

Из ИСПДн осуществляется вывод на печать сведений, содержащих персональные данные субъектов ПДн. Отпечатанные сведения хранятся в сейфе или передаются непосредственно субъекту ПДн согласно полномочий Администрации.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

Таблица 2 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администратор безопасности	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Сотрудник отдела по информатизации и программного обеспечения

	конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.		
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Приложение №3 к постановлению администрации ЕМР № 931 от 15.07.2014 г.

3 Модель вероятного нарушителя информационной безопасности

3.1 Описание возможных нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.
- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);

- пользователи ИСПДн (категория II);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИСПДн ТБ, но не имеющие права доступа к ресурсам (категория III);
- обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория IV);

уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория V).

На лиц I категории возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн ТБ, включая средства защиты, используемые в конкретных АС, 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 ИБ. 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.

На лиц II категории возложены задачи по использованию программно-аппаратных средств и баз данных ИСПДн. Пользователи потенциально могут реализовывать угрозы ИБ 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 АС, в соответствии с установленными для них полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-V относятся к вероятным нарушителям.

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

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки.

К внешним нарушителям могут относиться:

- бывшие сотрудники – администраторы или пользователи ИСПД (категория VI);

- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке (категория VII).

Лица категории VI 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 ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категории VII могут быть знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, но не знакомы с применяемыми принципами и концепциями безопасности на объекте ИСПДн. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категорий VI и VII потенциально могут реализовывать угрозы ИБ, используя возможности по несанкционированному доступу к защищаемой информации по каналам связи, обрабатываемой и хранимой в ИСПДн.

Предполагается, что лица категорий VI и VII относятся к вероятным нарушителям.

3.2 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- информации о назначения и общих характеристиках ИСПДн;
- информация, полученная из эксплуатационной документации;
- информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в СЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категорий III - VII не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категорий V – VI обладают чувствительной информацией об ИСПДн и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ИСПДн.

Организационными мерами предполагается исключить доступ лиц категории V к техническим и программным средствам ИСПД в момент обработки с использованием этих средств защищаемой информации.

Предполагается полностью исключить доступ лиц категорий VI – VII к техническим и программным средствам ИСПДн.

Таким образом, наиболее информированными об АС являются лица категорий V – VI.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания необходимых условий безопасности персональных данных предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

3.3. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение.

Предполагается что содержание и объем персональных данных, находящихся в ИСПДн не достаточны для мотивации применения нарушителем специально разработанных технических средства и программного обеспечения.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объекте ИСПДн конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, доступные в свободной продаже, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории V-VII.

3.4. Описание объектов и целей реализации угроз информационной безопасности

Основными информационными ресурсами, обрабатываемыми в ИСПДн являются следующие:

1. Целевая информация:

- персональные данные сотрудников;

2. Технологическая информация:

- защищаемая управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- защищаемая технологическая информация средств доступа к системам управления ИСПДн (аутентификационная информация и др.);

- информационные ресурсы ИСПДн на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами ИСПДн (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
- информация о СЗПДн, их структуре, принципах и технических решениях защиты;
- информационные ресурсы ИСПДн ТБ (базы данных и файлы), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах.

3. Программное обеспечение:

- программные информационные ресурсы ИСПДн, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами ИСПДн, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств защиты.

4.Предполагается, что не являются объектами реализации угроз:

- технические каналы утечки информации;
- сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- источники и цепи электропитания;
- цепи заземления.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

3.5 Описание каналов реализации угроз информационной безопасности

Возможными каналами реализации угроз информационной безопасности являются:

- каналы доступа, образованные с использованием специально разработанных технических средств и программного обеспечения.

Предполагается, что не являются каналами реализации угроз:

- технические каналы утечки;
- сигнальные цепи;
- источники и цепи электропитания;
- цепи заземления;
- каналы активного воздействия на технические средства с помощью облучения.

3.6 Основные способы реализации угроз информационной безопасности

При определении основных способов реализации угроз информационной безопасности ресурсов ИСПДн, учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла ИСПДн, компонентов, условий функционирования ИСПДн, а также - предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности ИСПДн:

1) несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн и недостатков механизмов разграничения доступа;

2) негативные воздействия на программно-технические компоненты ИСПДн ТБ вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;

3) маскировка под администратора ИСПДн, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых ИСПДн;

4) осуществление прямого хищения (утраты) элементов ИСПДн, носителей информации и производственных отходов (распечаток, списанных носителей);

5) компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых ИСПДн;

6) методы социальной инженерии для получения сведений об ИСПДн, способствующих созданию благоприятных условий для применения других методов;

7) использование оставленных без присмотра незаблокированных средств администрирования ИСПДн и АРМ;

8) сбои и отказы программно-технических компонентов ИСПДн;

9) внесение неисправностей, уничтожение технических и программно-технических компонентов ИСПДн путем непосредственного физического воздействия;

10) осуществление несанкционированного доступа к информации при ее передаче.

4. Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3 – Исходный уровень защищенности

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	Высокий
2	По наличию соединения с сетями общего пользования	Средний
3	По встроенным (легальным) операциям с записями баз персональных данных	Низкий
4	По разграничению доступа к персональным данным	Средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
6	По уровню (обезличивания) ПДн	Низкий
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокая

ИСПДн имеет ***средний*** уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности $Y_1 = 5$.

5. Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

5.1. Угрозы утечки информации по техническим каналам

5.1.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятна**.

5.1.2. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

В здании Администрации введен контроль доступа в контролируемую зону, АРМ с ИСПДн на окнах установлены шторы, что практически исключен визуальный просмотр посторонними лицами информации на мониторе. Вывод на печать ПДн осуществляется только в рамка исполнения полномочий Администрации. Отпечатанные сведения хранятся в сейфе или передаются непосредственно субъекту ПДн согласно исполнения полномочий Администрации..

Вероятность реализации угрозы – **маловероятна**.

5.1.3Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса **маловероятны**, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся на большом расстоянии от ее границы и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

5.2. Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

нарушению конфиденциальности (копирование, неправомерное распространение);

нарушению целостности (уничтожение, изменение);

нарушению доступности (блокирование).

5.2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

5.2.1.1.Кража ПЭВМ.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В здании Администрации введен круглосуточный контроль доступа в контролируемую зону, двери, закрываются на замок, вынос компьютерный техники за пределы здания возможен только по специальным пропускам.

Вероятность реализации угрозы – **маловероятной**.

5.2.1.2. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В здании Администрации Смоленской области №1 введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы – **маловероятна**.

5.2.1.3. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В здании Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и паролей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы – **маловероятна**.

5.2.1.4.Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В здании Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

5.2.1.5. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В здании Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

5.2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы – **маловероятна**.

5.2.1.7. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В здании Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – **низкая вероятность**.

5.2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

5.2.2.1. Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая вероятность**.

5.2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Разработку и сопровождение программного обеспечения ИСПДн осуществляет доверенная организация.

Вероятность реализации угрозы – ***маловероятна***.

5.2.2.3. Установка ПО не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все пользователи проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – **средняя вероятность**.

5.2.3 .Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

5.2.3.1. Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **средняя вероятность**.

5.2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В Администрации резервное копирование обрабатываемых ПДн не осуществляется.

Вероятность реализации угрозы – **высокая вероятность**.

5.2.3.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятна**.

5.2.3.4. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **средняя вероятность**.

5.2.3.5. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В Администрации ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – **маловероятна**.

5.2.3.6.Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Администрации установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна**.

5.2.4. Угрозы преднамеренных действий внутренних нарушителей

5.2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В здании Администрации введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

5.2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Администрации пользователи осведомлены о порядке работы с персональными данными, а так же подписали Соглашение о неразглашении.

Вероятность реализации угрозы – **маловероятна**.

5.2.5. Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;

- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

5.2.5.1. Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

- изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
- перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

В ИСПДн ТБ передача информации по каналам связи не осуществляется.

Перехват за переделами контролируемой зоны.
Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внешними нарушителями
Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями.
Вероятность реализации угрозы – **маловероятна**.

5.2.5.2. Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Вероятность реализации угрозы – **высокая вероятность**.

5.2.5.3. Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В Администрации применяются стойкие пароли.

Вероятность реализации угрозы – **маловероятна**.

5.2.5.4. Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

В ИСПДн ТБ не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

5.2.5.5. Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

В ИСПДн не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

5.2.5.6. Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

В ИСПДн ТБ не осуществляется межсетевое взаимодействие.

Вероятность реализации угрозы – **маловероятна**.

5.2.5.7. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

5.2.5.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

5.2.5.9. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – **маловероятно**.

6. Реализуемость угроз

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$

Оценка реализуемости УБПДн представлена в таблице.

Таблица 4 – Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,35	средняя
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,5	средняя
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа	0,5	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,75	высокая
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая
2.3.4. Выход из строя аппаратно-	0,5	средняя

программных средств		
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0,25	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,25	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0,25	низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,75	высокая
2.5.3.Угрозы выявления паролей по сети	0,25	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,25	низкая
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,25	низкая

7. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

- **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Таблица 5 – Опасность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	Низкая
1.2. Угрозы утечки видовой информации	Низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	Низкая
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	Низкая
2.1.2. Кража носителей информации	Низкая
2.1.3. Кража ключей и атрибутов доступа	Низкая
2.1.4. Кражи, модификации, уничтожения информации	Низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая
2.1.7. Несанкционированное отключение средств защиты	Низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	Низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	Низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая
2.3.3. Непреднамеренное отключение средств защиты	Низкая
2.3.4. Выход из строя аппаратно-программных средств	Низкая
2.3.5. Сбой системы электроснабжения	Низкая
2.3.6. Стихийное бедствие	Низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	Низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая
2.5.Угрозы несанкционированного доступа по каналам связи.	

2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	Низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	Низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Низкая
2.5.3.Угрозы выявления паролей по сети	Низкая
2.5.4.Угрозы навязывание ложного маршрута сети	Низкая
2.5.5.Угрозы подмены доверенного объекта в сети	Низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	Низкая
2.5.8.Угрозы удаленного запуска приложений	Низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	Низкая

8. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6 – Правила определения актуальности УБПДн

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 7 – Актуальность УБПДн

Тип угроз безопасности ПДн	Актуальность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	Не актуальная
1.2. Угрозы утечки видовой информации	Не актуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	Не актуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	Не актуальная

2.1.2. Кража носителей информации	Не актуальная
2.1.3. Кража ключей и атрибутов доступа	Не актуальная
2.1.4. Кражи, модификации, уничтожения информации	Не актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Не актуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Не актуальная
2.1.7. Несанкционированное отключение средств защиты	Не актуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	Не актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Не актуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Не актуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	Не актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Актуальная
2.3.3. Непреднамеренное отключение средств защиты	Не актуальная
2.3.4. Выход из строя аппаратно-программных средств	Не актуальная
2.3.5. Сбой системы электроснабжения	Не актуальная
2.3.6. Стихийное бедствие	Не актуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	Не актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Не актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	Не актуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	Не актуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Не актуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Не актуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Актуальная
2.5.3.Угрозы выявления паролей по сети	Не актуальная
2.5.4.Угрозы навязывание ложного маршрута сети	Не актуальная
2.5.5.Угрозы подмены доверенного объекта в сети	Не актуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Не актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	Не актуальная

2.5.8.Угрозы удаленного запуска приложений	Не актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	Не актуальная

Были выявлены следующие актуальные угрозы:

- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

- Резервное копирование данных ИСПДн ТБ.

9. Модель угроз безопасности

Исходный класс защищенности – средний (Y1=5).

Таблица 8 – Угрозы безопасности

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятна	Низкая	Низкая	Неактуальная	Закрытые окна, двери.	Инструкция пользователя Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятна	Низкая	Низкая	Неактуальная	Жалюзи на окна Расположение монитора	Инструкция пользователя Технологический процесс
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятна	Низкая	Низкая	Неактуальная		Неактуальная
2. Угрозы несанкционированного доступа к информации						
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
2.1.1. Кража ПЭВМ	Маловероятна	Низкая	Низкая	Неактуальная		Пропускной режим Охрана
2.1.2. Кража носителей информации	Маловероятна	Низкая	Низкая	Неактуальная	Хранение в сейфе Система защиты от НСД	Пропускной режим Охрана Акт установки средств защиты Учет носителей информации Инструкция пользователя
2.1.3. Кража ключей доступа	Маловероятна	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя

2.1.4. Кражи, модификации, уничтожения информации.	Маловероятна	Низкая	Низкая	Неактуальная	Система защиты от НСД	Пропускной режим Охрана Акт установки средств защиты
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятна	Низкая	Низкая	Неактуальная		Пропускной режим Охрана
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Маловероятна	Низкая	Низкая	Неактуальная	Система защиты от НСД	Ремонт допущенными сотрудниками учреждения
2.1.7. Несанкционированное отключение средств защиты	Низкая вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности Технологический процесс обработки
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						
2.2.1. Действия вредоносных программ (вирусов)	Низкая вероятность	Средняя	Низкая	Неактуальная	Антивирусное ПО	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки Инструкция по антивирусной защите
2.2.2. Недекларированные	Маловероятна	Низкая	Низкая	Неактуальная	Настройка средств	Приобретение у

возможности системного ПО и ПО для обработки персональных данных					защиты	доверенной организации
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Средняя вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности Технологический процесс обработки
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования испдн и сзпдн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Средняя вероятность	Средняя	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя Инструкция администратора безопасности Журнал учета паролей
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Высокая вероятность	Высокая	Низкая	Актуальная	Настройка средств защиты	Инструкция пользователя
2.3.3. Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности Настройка средств защиты	Инструкция пользователя Инструкция администратора безопасности Инструкция по антивирусной защите
2.3.4. Выход из строя	Средняя	Средняя	Низкая	Неактуальная		Неактуальная

аппаратно-программных средств	вероятность					
2.3.5. Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	
2.3.6. Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальная	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятна	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Маловероятна	Низкая	Низкая	Неактуальная		Обязательство о не разглашении Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:						
2.5.1.1. Перехват за переделами с контролируемой зоны;	Маловероятна	Низкая	Низкая	Неактуальная		Неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятна	Низкая	Низкая	Неактуальная		Неактуальная

2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятна	Низкая	Низкая	Неактуальная		Неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Высокая вероятность	Высокая	Низкая	Актуальная	Сетевой экран	
2.5.3. Угрозы выявления паролей по сети.	Маловероятна	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятна	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятна	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	Сетевой экран	
2.5.9. Угрозы внедрения по	Маловероятно	Низкая	Низкая	Неактуальная	Сетевой экран	

сети вредоносных программ.					Антивирусное ПО	

10. Заключение

Ввиду исключительной роли в ИСПДн лиц категорий I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Лица категорий III-VII относятся к вероятным нарушителям.

Среди лиц категорий III-VII наиболее опасными вероятными нарушителями являются лица категорий V-VI (уполномоченный персонал разработчиков ИСПДн ТБ, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн, бывшие сотрудники).

На основании проведенного анализа можно сделать вывод что вероятный нарушитель относится к классу Н1.

Представленная модель угроз для ИСПДн должна использоваться при формировании обоснованных требований информационной безопасности и проектировании ИСПД.

Для предотвращения возможности реализации актуальных угроз безопасности необходимо:

- -организовать резервное копирование информации, хранящейся в ИСПДн Администрации;
- -создать комиссию по защите ПДн и привести в соответствие Российскому законодательству нормативные акты Администрации.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, исходя из анализа угроз безопасности ПДн, а так же учитывая то, что:

- ИСПДн Администрации является специальной информационной системой,
- в ИСПД ТБ одновременно обрабатываются данные менее 1000 субъектов персональных данных,
- нарушение безопасности персональных данных, обрабатываемых в ИСПД, может привести к незначительным негативным последствиям для субъектов персональных данных,
- класс информационной системы определяется по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных,
- можно определить, что **ИСПДн Администрации классифицируется, как специальная ИСПДн класса К3.**

Аттестация ИСПДн Администрации не требуется.

Приложение №2 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Перечень персональных данных, обрабатываемых в администрации Ершовского муниципального района Саратовской области.

№	Наименование (вид) ПДн	Содержание ПДн	Категория ПДн	Источник получения ПДн	Основание для обработки ПДн	Технологический процесс, использующий вид ПДн	Срок хранения, условия прекращения обработки	Общедоступность
1. Субъект ПДн граждане, состоящие с Администрацией в отношениях, регулируемых трудовым законодательством, законодательством о муниципальной службе в том числе граждане, являющиеся кандидатами на включение во внешний кадровый резерв.								
1.	Первичные учетные данные работников	ФИО работника	3 категория	-Субъект ПДн -Паспорт -СНИЛС -ИНН -Диплом об образовании -Заявление о приеме на работу -Трудовая книжка - д.р.	Трудовое законодательство РФ, согласие субъекта ПДн.	-Прием на работу -Увольнение -Начисление зарплаты -Начисление премии -Заключение договора -Изменение данных -Выдача справки -Расторжение договора	На период работы, и 75 лет после увольнения	Нет

2.	Сведения о занимаемой должности	- Наименование организации - Наименование структурного подразделения - наименование занимаемой должности	3 категория	-Субъект ПДн -Трудовой договор -Трудовая книжка - д.р.	Трудовое законодательство РФ, согласие субъекта ПДн.	-Прием на работу -Увольнение -Начисление зарплаты -Начисление премии	На период работы, и 75 лет после увольнения	Нет
3.	Финансовое состояние работника	Сведения о текущем должностном окладе	3 категория	-Субъект ПДн -Трудовой договор -Распоряжение о премиях - д.р.	Трудовое законодательство РФ, согласие субъекта ПДн.	-Прием на работу -Начисление зарплаты -Начисление премии	На период работы, и 75 лет после увольнения	Нет
4.	Сведения о реквизитах работника	-Дата рождения -Адрес прописки -ИНН -Данные паспорта -СНИЛС	3 категория	-Субъект ПДн -Диплом -Паспорт - д.р.	Трудовое законодательство РФ, согласие субъекта ПДн.	-Прием на работу -Начисление зарплаты -Начисление премии	На период работы, и 75 лет после увольнения	Нет

5.	Дополнительные сведения о работнике	-Образование -Дети -Семейное положение	3 категория	-Субъект ПДн -Диплом -Паспорт -Свидетельство о рождении ребенка - Свидетельство о браке. - д.р.	Трудовое законодательство РФ, согласие субъекта ПДн.	-Прием на работу -Начисление зарплаты -Начисление премии	На период работы, и 75 лет после увольнения	Нет
2. Субъект ПДн граждане, состоящие с Администрацией в гражданско-правовых отношениях в том числе граждане, в связи с реализацией полномочий органа местного самоуправления и (или) предоставлением муниципальных услуг.								
1.	Первичные учетные данные	ФИО	3 категория	-Субъект ПДн -Соглашение -Обращение - д.р.	-Согласие субъекта ПДн -Условия договора -Обращение	-Заключение договора -Изменение данных -Выдача справки -Расторжение договора -Ответ на обращение	5 лет после расторжения договора, предоставления услуги или ответа на обращение	Нет
2.	Сведения о реквизитах	-Дата рождения -Адрес прописки -ИНН -Данные паспорта -СНИЛС	3 категория	-Субъект ПДн - Соглашение -Обращение - д.р.	-Согласие субъекта ПДн -Условия договора -Обращение	-Заключение договора -Изменение данных -Выдача справки -Расторжение договора -Ответ на обращение	5 лет после расторжения договора, предоставления услуги или ответа на обращение	Нет

3.	Дополнительные сведения	- Образование -Дети -Семейное положение	3 категория	-Субъект ПДн - Соглашение -Обращение - д.р.	-Согласие субъекта ПДн -Условия договора -Обращение	-Заключение договора -Изменение данных -Выдача справки -Расторжение договора -Ответ на обращение	5 лет после расторжения договора, предоставления услуги или ответа на обращение	Нет

Приложение №3 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Перечень лиц, должностей допущенных к обработке персональных данных.

№	ФИО сотрудника	Должность
1.	ФИО	должность отдела по информатизации и программному обеспечению
2.	ФИО	должность отдела по информатизации и программному обеспечению
3.	ФИО	должность отдела кадров, делопроизводства и контроля
4.	ФИО	должность отдела кадров, делопроизводства и контроля
5.	ФИО	должность службы субсидий
6.	ФИО	должность службы субсидий
7.	ФИО	должность отдела по аграрной политике и природопользованию
8.	ФИО	должность отдела по аграрной политике и природопользованию
9.	ФИО	должность отдела по управлению муниципальным имуществом, земельным ресурсам и экономической политики
10.	ФИО	должность отдела по организационным вопросам и взаимодействию с ОМСУ
11.	ФИО	должность отдела по управлению муниципальным имуществом, земельным ресурсам и экономической политики
12.	ФИО	должность отдела образования
13.	ФИО	должность отдела ЖКХ, транспорта и связи
14.	ФИО	должность отдела ЖКХ, транспорта и связи
15.	ФИО	должность сектора опеки и попечительства

Приложение №4 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Перечень информационных систем по обработке персональных данных.

№	Информационная система по обработке персональных данных	Место установки
Региональные системы		
1.	ИСПДн	ул.Интернациональная, 7, каб. №
2.	ИСПДн	ул.Интернациональная, 7, каб. №
3.	ИСПДн	ул.Интернациональная, 7, каб. №
4.	ИСПДн	ул.Интернациональная, 7, каб. №
Федеральные системы		
5.	ИСПДн	ул.Интернациональная, 7, каб. №
6.	ИСПДн	ул.Интернациональная, 7, каб. №
7.	ИСПДн	ул.Интернациональная, 7, каб. №
8.	ИСПДн	ул.Интернациональная, 7, каб. №
9.	ИСПДн	ул.Интернациональная, 7, каб.№
10.	ИСПДн	ул.Интернациональная, 7, каб.№
11.	ИСПДн	ул.Интернациональная, 7, каб.№
12.	ИСПДн	ул.Интернациональная, 7, каб.№
13.	ИСПДн	ул.Интернациональная, 7, каб.№
14.	ИСПДн	ул.Краснопартизанская, 7 каб.№

Приложение №5 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Политика администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных.

1. Общие положения

1.1. Настоящая Политика администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных (далее по тексту – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона Российской Федерации «О персональных данных» № 152-ФЗ от 27 июля 2006 года (ред. от 02.07.2021 N 331-ФЗ) а также иных нормативно-правовых актов Российской Федерации в области защиты и обработки персональных данных и действует в отношении всех персональных данных (далее по тексту – Данных), которые администрация Ершовского муниципального района Саратовской области и отраслевые (функциональные) органы администрация Ершовского муниципального района Саратовской области, не являющихся юридическими лицами (далее по тексту – Оператор, Администрация) может получить от субъекта персональных данных, в связи с реализацией полномочий органа местного самоуправления, в том числе предоставлением муниципальных услуг, рассмотрением обращений граждан Российской Федерации в соответствии с законодательством, гражданско-правовому договору, а так же от субъекта персональных данных, состоящего с Администрацией в отношениях, регулируемых трудовым законодательством (далее по тексту – Работник, Кандидат на занимаемую должность).

1.2. Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ “О персональных данных”, Постановления Правительства Российской Федерации от 15.09. 2008 N 687 “Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации”, постановления Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", иных нормативных документов уполномоченных органов.

1.3. Изменение Политики

1.3.1. Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего

обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.3.2. Действующая редакция хранится в электронном виде на сайте Оператора по адресу: https://adminemr.ru

2. Термины, определения и принятые сокращения в Политике используются в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

-Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

-Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

-Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

-Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

-Персональные данные, сделанные общедоступными субъектом персональных данных – ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

-Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

-Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

-Оператор – организация, обрабатывающая персональные данные.

3.Обработка персональных данных

3.1. Получение ПД.

3.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

3.1.2. Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения ПД, характере подлежащих получению ПД, перечне действий с ПД, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать письменное согласие на их получение.

3.1.3. Документы, содержащие ПД создаются путем:

-копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

-внесения сведений в учетные формы;

-получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.)

3.2. Обработка ПД

3.2.1. Обработка персональных данных осуществляется:

-с согласия субъекта персональных данных на обработку его персональных данных;

-в случаях, реализацией полномочий органа местного самоуправления, в том числе предоставлением муниципальных услуг;

-в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

3.2.2 Цели обработки персональных данных:

-Исполнение условий трудового договора (служебного контракта) и осуществление прав и обязанностей в соответствии с трудовым законодательством, законодательством о муниципальной службе;

-Рассмотрение обращений граждан Российской Федерации в соответствии с законодательством;

-Выполнение обязательств по гражданско-правовым договорам (контрактам) и иным соглашениям, заключаемым с Администрацией;

-Предоставление муниципальных услуг, реализация полномочий органа местного самоуправления;

-Создание общедоступных источников персональных данных.

3.2.3. Категории субъектов персональных данных. Оператором обрабатываются ПД следующих субъектов ПД:

-Граждане, состоящие с Администрацией в отношениях, регулируемых трудовым законодательством, законодательством о муниципальной службе;

-Граждане, являющиеся кандидатами на включение во внешний кадровый резерв Администрации;

-Граждане, персональные данные которых обрабатываются в связи с реализацией полномочий органа местного самоуправления, в том числе предоставлением муниципальных услуг;

-Граждане, состоящие с Администрацией в гражданско-правовых отношениях;

-Обработка персональных данных осуществляется с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие субъекта персональных данных должно отвечать требованиям, определенным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2.4. Перечень ПД, обрабатываемые Оператором перечислены в Приложении №2 к постановлению администрации ЕМР № 931 от 15.07.2014г.

3.2.5. Обработка персональных данных ведется:

-С использованием средств автоматизации;

-Без использования средств автоматизации

3.3. Хранение ПД

3.3.1. ПД Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.3.2. ПД, зафиксированные на бумажных носителях хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

3.3.3. ПД Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

3.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

3.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.4. Уничтожение ПД

3.4.1. Уничтожение документов (носителей), содержащих ПД производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

3.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.5. Передача ПД

3.5.1. Оператор передает ПД третьим лицам в следующих случаях:

-Субъект выразил свое согласие на такие действия;

-Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

3.5.2. Перечень лиц, которым передаются ПД. Третьи лица, которым передаются ПД:

-Пенсионный фонд РФ для учета (на законных основаниях);

-Налоговые органы РФ (на законных основаниях);

-Фонд социального страхования (на законных основаниях);

-Территориальный фонд обязательного медицинского страхования (на законных основаниях);

-Страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

-Банки для начисления заработной платы (на основании договора);

-Иные органы в случаях, установленных законодательством Российской Федерации.

4. Защита персональных данных

4.1. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

4.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

4.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, контрагентами и сторонними лицами.

4.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

4.5. Основными мерами защиты ПД, используемыми Оператором, являются:

-Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД;

-Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;

-Разработка политики в отношении обработки персональных данных;

-Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД;

-Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

-Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

-Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

-Сертифицированное программное средство защиты информации от несанкционированного доступа;

-Сертифицированные межсетевой экран и средство обнаружения вторжения;

-Соблюдаются условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ;

-Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

-Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

-Обучение работников Оператора непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

-Осуществление внутреннего контроля и аудита.

5. Основные права субъекта ПД и обязанности оператора

5.1. Основные права субъекта ПД Субъект имеет право на доступ к его персональным данным и следующим сведениям:

-подтверждение факта обработки ПД оператором;

-правовые основания и цели обработки ПД;

-цели и применяемые оператором способы обработки ПД;

-наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с оператором или на основании федерального закона;

-сроки обработки персональных данных, в том числе сроки их хранения;

-порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;

-наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;

-обращения к оператору и направлению ему запросов; - обжалование действий или бездействия оператора.

5.2. Обязанности Оператора Оператор обязан:

-при сборе ПД предоставить информацию об обработке ПД;

-в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;

-при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;

-опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;

-принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;

-давать ответы на запросы и обращения Субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.

Приложение №1 к Политике администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных.

Согласия на обработку персональных данных субъектов персональных данных

Я, _____ ,
фамилия, имя, отчество (при наличии)

зарегистрированный(ая) по адресу: _____

_____

паспорт серии_____ № _____, выдан _____

_____ ,
кем и когда выдан

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам администрации Ершовского муниципального района Саратовской области находящейся по адресу:

413503, Россия, Саратовская область, г. Ершов, ул. Интернациональная, 7

на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии), дата, место и причина изменения в случае их изменения);

2) число, месяц, год рождения;

3) место рождения;

4) сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5) сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация);

6) сведения об ученой степени, ученом звании;

7) сведения о профессиональной переподготовке и (или) повышении квалификации;

8) сведения о владении иностранными языками, степень владения;

9) сведения о классном чине гражданской службы Российской Федерации (дипломатическом ранге, классном чине юстиции, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде

гражданской службы (квалификационном разряде или классном чине муниципальной службы), кем и когда присвоены;

10) сведения о наличии или отсутствии судимости;

11) сведения об оформленных за период работы, службы, учебы допусках к государственной тайне;

12) сведения о трудовой деятельности (включая работу по совместительству, предпринимательскую и иную деятельность), военной службе;

13) сведения о государственных наградах, иных наградах и знаках отличия;

14) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших);

15) сведения о близких родственниках (отец, мать, братья, сестры и дети), а также супругах, в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (при наличии), с какого времени проживают за границей);

16) сведения о пребывании за границей (когда, где и с какой целью);

17) отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета;

18) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

19) номер контактного телефона или сведения о других способах связи;

20) вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его;

21) реквизиты паспорта гражданина Российской Федерации, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации (серия, номер, когда и кем выдан);

22) реквизиты страхового свидетельства обязательного пенсионного страхования;

23) идентификационный номер налогоплательщика;

24) реквизиты страхового медицинского полиса обязательного медицинского страхования;

25) реквизиты свидетельств государственной регистрации актов гражданского состояния;

26) сведения об отсутствии заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

27) сведения об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну;

28) личная фотография;

29) сведения о прохождении гражданской службы (работы), в том числе: дата, основания поступления на гражданскую службу (работу) и назначения на должность гражданской службы, дата, основания назначения, перевода, перемещения на иную должность гражданской службы (работы), наименование замещаемых должностей гражданской службы с указанием структурных подразделений, размера денежного содержания (заработной платы), результатов аттестации на соответствие замещаемой должности гражданской службы, а также сведения о прежнем месте работы;

30) сведения, содержащиеся в служебном контракте (трудовом договоре), дополнительных соглашениях к служебному контракту (трудовому договору);

31) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с исполнение условий трудового договора (служебного контракта) и осуществление прав и обязанностей в соответствии с трудовым законодательством, законодательством о муниципальной службе.

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока исполнения выше указанных отношений;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Администрация Ершовского муниципального района Саратовской области вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2—11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4) после прекращения непосредственно связанных с ним выше указанных отношений) персональные данные будут храниться в Администрация Ершовского муниципального района Саратовской области в течение предусмотренного законодательством Российской

Федерации и иными нормативными правовыми актами Российской Федерации срока хранения документов;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию Ершовского муниципального района Саратовской области функций, полномочий и обязанностей.

Дата начала обработки персональных данных: _____
число, месяц, год

_____
подпись

Приложение №2 к Политике администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных**.**

Согласия на обработку персональных данных субъектов персональных данных

Я, _____ ,
фамилия, имя, отчество (при наличии)

зарегистрированный(ая) по адресу: _____

_____

паспорт серии _____ № _____, выдан _____

_____ ,
кем и когда выдан

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам администрации Ершовского муниципального района Саратовской области находящейся по , адресу: 413503, Россия, Саратовская область, г. Ершов, ул. Интернациональная, 7

на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

-данные, необходимые для достижения целей, предусмотренных Постановлением администрации Ершовского муниципального района Саратовской области от 15.07.2014 г №931 "Об утверждении политики администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных":_____

_____

_____

—

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с*:_____

_____

_____

—

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока исполнения выше указанных отношений;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Администрация Ершовского муниципального района Саратовской области вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2—11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4) после прекращения непосредственно связанных с ним выше указанных отношений) персональные данные будут храниться в Администрация Ершовского муниципального района Саратовской области в течение предусмотренного законодательством Российской Федерации и иными нормативными правовыми актами Российской Федерации срока хранения документов;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию Ершовского муниципального района Саратовской области функций, полномочий и обязанностей.

Дата начала обработки персональных данных: _____
число, месяц, год

_____
подпись

*

1)Рассмотрение обращений граждан Российской Федерации в соответствии с законодательством;

2)Выполнение обязательств по гражданско-правовым договорам (контрактам) и иным соглашениям, заключаемым с Администрацией;

3)Предоставление муниципальных услуг, реализация полномочий органа местного самоуправления;

Приложение №3 к Политике администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных.

Разъяснение
субъекту персональных данных

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в администрацию Ершовского муниципального района Саратовской области.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в администрацию Ершовского муниципального района Саратовской области в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Приложение №6 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Правила работы с персональными данными для сотрудников администрации Ершовского муниципального района Саратовской области, в обязанности которых входит регистрация, рассмотрение запросов субъектов персональных данных, обработка и защита персональных данных.

1. Общие положения

1.1.Настоящие правила регистрации (учета) персональных данных их обработку и рассмотрения запросов субъектов персональных данных в администрации Ершовского муниципального района Саратовской области (далее по тексту –Администрация) устанавливают:

-особенности организации обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации;

-сроки обработки и хранения персональных данных;

-порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;

-единый порядок регистрации (учета) и рассмотрения запросов субъектов персональных данных или их представителей (далее по тексту – запросы).

1.2.В правилах используются понятия и термины, определенные Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

1.3.В Администрации осуществляется автоматизированная обработка персональных данных, а также обработка персональных данных без использования средств автоматизации.

1.4.Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также под роспись ознакомлены с настоящими правилами, положениями законодательства Российской Федерации, правовыми актами Администрации о порядке обработки персональных данных и требованиях к обеспечению безопасности персональных данных. Форма соответствующего листа ознакомления приводится в приложении к настоящим правилам.

2. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации

2.1.Порядок обработки персональных данных, осуществляемой без использования средств автоматизации, определяется постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и правовыми актами Администрации.

2.2.Обработка персональных данных без использования средств автоматизации осуществляется на материальных носителях информации (далее по тексту – материальные носители).

2.3.Персональные данные обособляются от иной информации путем фиксации их на отдельных материальных носителях.

2.4.Запрещается оставлять материальные носители без присмотра или передавать на хранение другим лицам, не имеющим на это полномочий.

2.5.Запрещается выносить из служебных помещений материальные носители.

2.6.Учет машинных съемных носителей информации осуществляется путем ведения журналов учета.

2.7.Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

2.8.В случае, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на этом носителе персональных данных или иной информации, принимаются следующие меры:

2.8.1.При необходимости использования или распространения определенных персональных данных осуществляется их копирование с целью последующего использования копии.

2.8.2.При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или копированию.

2.9.Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.Особенности обработки персональных данных с использованием средств автоматизации.

3.1. Основы обработки персональных данных, осуществляемой с использованием средств автоматизации, определяются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 21.03.2012 № 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», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также другими принятыми нормативно-методическими и организационно-распорядительными документами Администрации.

3.2.В Администрации один из заместителей руководителя структурного подразделения назначается ответственным за обеспечение безопасности информации ограниченного доступа на объектах вычислительной техники и осуществляет непосредственное руководство работами по защите информации.

3.3.Для обеспечения безопасности персональных данных при их обработке в информационных системах выполняются мероприятия, предусмотренные постановлением администрации Ершовского муниципального района Саратовской области от 15.07.2014 № 931 «Об утверждении политики администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных».

3.4.Лица, ответственные за безопасность персональных данных при их обработке в информационных системах, обеспечивают, в том числе:

3.4.1. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

3.4.2.Недопущение воздействия на программно-аппаратные средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

3.4.3.Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа.

3.4.4.Постоянный контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

3.4.5.Знание и соблюдение условий использования средств защиты информации лицами, осуществляющими обработку персональных данных.

3.4.6.Незамедлительное приостановление предоставления доступа к персональным данным лицам, осуществляющим обработку персональных данных, при обнаружении нарушений.

3.4.7.Незамедлительное доведение информации о фактах нарушений функционирования системы защиты информации до руководителя органа с целью последующего уведомления лица, ответственного за организацию

обработки персональных данных в Администрации, составление заключений по фактам нарушений.

3.5.Запрещается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

-настроенных сертифицированных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств, в соответствии с требованиями безопасности информации;

-утвержденных организационно-распорядительных документов по информационной системе персональных данных;

-приказа о вводе в эксплуатацию информационной системы персональных данных с назначением ответственных лиц за безопасность информации.

3.6.В информационных системах персональных данных Администрации не осуществляется обработка:

-биометрических персональных данных;

-специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

В случае принятия решения об обработке биометрических персональных данных и специальных категорий персональных данных, такие данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или в случаях, установленных законодательством Российской Федерации.

3.7.Трансграничная передача персональных данных Администрацией не осуществляется. В случае принятия решения о трансграничной передаче персональных данных такие данные могут передаваться только при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных или в случаях, установленных законодательством Российской Федерации, предусматривающих трансграничную передачу персональных данных без письменного согласия субъекта персональных данных.

3.8.Сведения об информационных системах персональных данных Администрации содержатся в Перечень информационных систем по обработке персональных данных Администрации, утвержденном постановлением администрации Ершовского муниципального района Саратовской области от 15.07.2014 № 931 «Об утверждении политики администрации Ершовского муниципального района Саратовской области в отношении обработки и защиты персональных данных».

4. Сроки обработки и хранения персональных данных

4.1. Сроки обработки персональных данных определяются в соответствии с целью обработки. Персональные данные подлежат уничтожению по достижении цели обработки персональных данных, если иное не предусмотрено федеральным законодательством.

4.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

4.3.Сроки обработки и хранения персональных данных в информационных системах персональных данных устанавливаются правовыми актами Администрации, определяющими порядок их эксплуатации.

4.4.Сроки обработки и хранения персональных данных на бумажных носителях определяются:

4.4.1.При обработке персональных данных муниципальных служащих Администрации, иных сотрудников Администрации, руководителей муниципальных предприятий и муниципальных учреждений Ершовского района требованиями трудового законодательства, законодательства о муниципальной службе и законодательства об архивном деле.

4.4.2.При обработке персональных данных граждан, обратившихся в Администрацию лично либо направивших индивидуальные или коллективные письменные обращения, а также в целях предоставления муниципальных услуг и исполнения муниципальных функций, требованиями Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», законодательства об архивном деле, административными регламентами и иными правовыми актами Администрации.

5.Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

5.1.Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2.Лица, осуществляющие обработку персональных данных, в рамках своих полномочий, проводят систематические проверки и выделение документов на бумажных и материальных съемных носителях, а также данных, хранящихся в информационных системах персональных данных и содержащих персональные данные с истекшими сроками хранения, подлежащих уничтожению.

5.3.Решение об уничтожении документов, содержащих персональные данные, принимают руководители органов, в которых осуществляется обработка персональных данных.

5.4.По окончании процедуры уничтожения составляется соответствующий акт с указанием даты и основания уничтожения.

6. Права субъектов персональных данных.

Субъект персональных данных имеет право на:

6.1.Получение информации, касающейся обработки его персональных данных, предусмотренной частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Данное право может быть ограничено в случаях, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.2.Уточнение персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.3.Обжалование действий (бездействия) сотрудников Администрации в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке, если субъект персональных данных считает, что органы осуществляют обработку его персональных данных с нарушением законодательства Российской Федерации или иным образом нарушают его права и свободы.

71

6.4.Защиту своих прав и законных интересов в судебном порядке.

7. Порядок рассмотрения запросов субъектов персональных данных или их представителей

7.1.Сведения, касающиеся обработки персональных данных, предусмотренные частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предоставляются субъекту персональных данных или его представителю при направлении ими запроса или обращении в Администрацию.

7.2.Запрос должен содержать следующие сведения:

-фамилию, имя, отчество субъекта персональных данных, а также, в случае направления запроса представителем субъекта персональных данных, его фамилию, имя, отчество;

-сведения о документе, удостоверяющем личность субъекта персональных данных или его представителя;

-сведения, подтверждающие факт обработки персональных данных Администрацией;

-подпись субъекта персональных данных или его представителя;

-доверенность, оформленную в установленном порядке, в случае направления запроса представителем субъекта персональных данных.

7.3.Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.4.Запрос регистрируется в течение трех дней со дня его поступления.

7.5.Запросы, поступающие в адрес главы Ершовского района, первого заместителя главы Администрации, заместителей главы Администрации, руководителя аппарата главы Администрации, регистрируются сотрудниками отдела кадров, делопроизводства и контроля Администрации и передаются согласно резолюции вышеуказанных лиц в отраслевые (функциональные) отделы Администрации.

7.6.Запросы, поступающие в адрес руководителей органов, регистрируются сотрудниками данных органов, ответственными за делопроизводство.

7.7.Сведения по запросу либо отказ в предоставлении сведений направляются субъекту персональных данных или его представителю в срок, не превышающий тридцати дней с даты получения запроса.

7.8.Лицо, осуществляющее подготовку ответа на запрос, обязано:

-разобраться в существе запроса, в случае необходимости истребовать дополнительные материалы или осуществить проверку фактов, изложенных в запросе;

-принять законные, обоснованные и мотивированные решения и обеспечить их своевременное и надлежащее исполнение;

-сообщить субъекту персональных данных или его представителю о решениях, принятых по его запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса разъяснить порядок обжалования этого решения.

7.9.В ответе субъекту персональных данных или его представителю сообщается информация о наличии персональных данных, а также предоставляется возможность ознакомления с персональными данными при личном обращении.

7.10.Отказ в предоставлении информации о наличии персональных данных или в предоставлении возможности ознакомления с персональными данными должен содержать законное основание для такого отказа.

7.11.Сведения предоставляются субъекту персональных данных или его представителю в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких данных.

7.12.Возможность ознакомления с персональными данными предоставляется субъекту персональных данных или его представителю на безвозмездной основе.

7.13.В случае если сведения были предоставлены для ознакомления субъекту персональных данных или его представителю по его запросу, субъект персональных данных вправе направить повторный запрос не ранее чем через 30 дней после первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.14.Субъект персональных данных вправе направить повторный запрос до истечения срока, указанного в подпункте 7.13, в случае если сведения не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

7.15.Администрация отказывают субъекту персональных данных или его представителю в выполнении повторного запроса, если запрос не соответствует условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с указанием оснований для отказа.

7.16.В случае предоставления субъектом персональных данных или его представителем сведений о том, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, лицо, обрабатывающее персональные данные, обязано уничтожить такие персональные данные на основании приказа руководителя структурного подразделения администрации города Нижнего Новгорода.

7.17.В случае поступления сведений о неправомерной обработке персональных данных от субъекта персональных данных, его представителя или уполномоченного органа по защите прав субъектов персональных данных, лицо, обрабатывающее персональные данные, обязано приостановить обработку неправомерно обрабатываемых персональных данных, с момента получения запроса на период проведения проверки.

7.18. В случае выявления неправомерной обработки персональных данных лицо, обрабатывающее персональные данные, в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку таких персональных данных. В случае невозможности обеспечения правомерности обработки персональных данных, лицо, обрабатывающее персональные данные, обязано уничтожить такие персональные данные либо обеспечить их уничтожение в установленный законом срок на основании приказа руководителя структурного подразделения Администрации. Об устранении допущенных нарушений или об уничтожении персональных данных органы обязаны уведомить субъекта персональных данных или его представителя, а также в случае, если запрос был направлен уполномоченным органом по защите прав субъектов персональных данных, уведомить указанный орган.

7.19.В случае предоставления субъектом персональных данных, его представителем либо органом по защите прав субъектов персональных данных сведений о том, что персональные данные субъекта являются неполными, неточными или неактуальными, лицо, обрабатывающее персональные данные, обязано приостановить обработку таких персональных данных с момента получения запроса на период проведения проверки, если это не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.20.В случае подтверждения факта неточности персональных данных лицо, обрабатывающее персональные данные, на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязано уточнить персональные данные в срок, не превышающий семи рабочих дней со дня представления сведений, и возобновить обработку персональных данных. Администрации обязана уведомить субъекта персональных данных или его представителя о внесенных

изменениях, а также принять меры для уведомления третьих лиц, которым эти данные были переданы.

7.21.При необходимости для проверки фактов, изложенных в запросах, организуются служебные проверки в соответствии с правовыми актами Администрации или приказами руководителей подведомственных органов.

7.22.По результатам служебной проверки составляется мотивированное заключение (акт), которое должно содержать объективный анализ собранных материалов. Если по результатам проверки выявлены факты совершения лицом, осуществляющим обработку персональных данных, действия (бездействия), содержащего признаки административного правонарушения или преступления, материалы передаются в правоохранительные органы. Результаты служебной проверки докладываются лицу, ответственному за организацию обработки персональных данных в Администрации.

7.23.Запрос считается рассмотренным, если в ответе на запрос рассмотрены все поставленные в нем вопросы, приняты необходимые меры, и субъекту персональных данных или его представителю дан исчерпывающий ответ.

7.24.Лицо, ответственное за организацию обработки персональных данных в Администрации, осуществляет контроль за соблюдением порядка рассмотрения запросов:

-сроков исполнения поручений по запросам;

-полноты рассмотрения запросов;

-объективности проверки фактов, изложенных в запросах;

-законности и обоснованности принятых решений;

-своевременности исполнения принятых решений;

-своевременности направления ответов заявителям.

7.25.Нарушение настоящих правил влечет ответственность, предусмотренную законодательством Российской Федерации.

Приложение к Правилам работы с персональными данными для сотрудников администрации Ершовского муниципального района Саратовской области

ЛИСТ ОЗНАКОМЛЕНИЯ

лица, осуществляющего регистрацию, рассмотрение запросов субъектов персональных данных, обработку и защиту персональных данных, с положениями законодательства РФ, правовыми актами Администрации о порядке регистрации, рассмотрении запросов субъектов персональных данных, обработке и защите персональных данных.

Я, _____,
(фамилия, имя, отчество)

_____

_____
(должность)

_____,
ознакомлен(а) с положениями законодательства Российской Федерации и правовыми актами Администрации о порядке регистрации, рассмотрении запросов субъектов персональных данных, обработке и защите персональных данных.

Мною изучены положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Трудового кодекса Российской Федерации, постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», правовых актов Администрации об обработке персональных данных.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, обязуюсь не раскрывать третьим лицам и не распространять персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей.

Ответственность и права, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснены.

«____»_____20___г. _____ _____
(подпись) (расшифровка подписи)

71

Приложение №7 к постановлению администрации Ершовского муниципального района от 21.07.2021 № 460

Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.Общие положения

1. 1.Положение об организации режима обеспечения безопасности помещений администрации Ершовского муниципального района Саратовской области и отраслевых (функциональных) органов администрации Ершовского муниципального района Саратовской области, не являющихся юридическими лицами (далее по тексту – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее по тексту – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и устанавливает единые требования доступу к помещениям Администрации в которых ведется обработка персональных данных в целях предотвращения нарушения прав субъектов персональных данных и обеспечения соблюдения требований законодательства о персональных данных.

1.2.Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной и системой контроля и управления доступом.

2.Границы контролируемой зоны

2.1.Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

План-схема контролируемой зоны помещений по адресу Саратовская область, г.Ершов, ул.Интернациональная, 7 приведена в приложении 1 к настоящему положению.

2.2.Размещение информационных систем персональных данных, специального оборудования осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

3.Порядок доступа в помещения

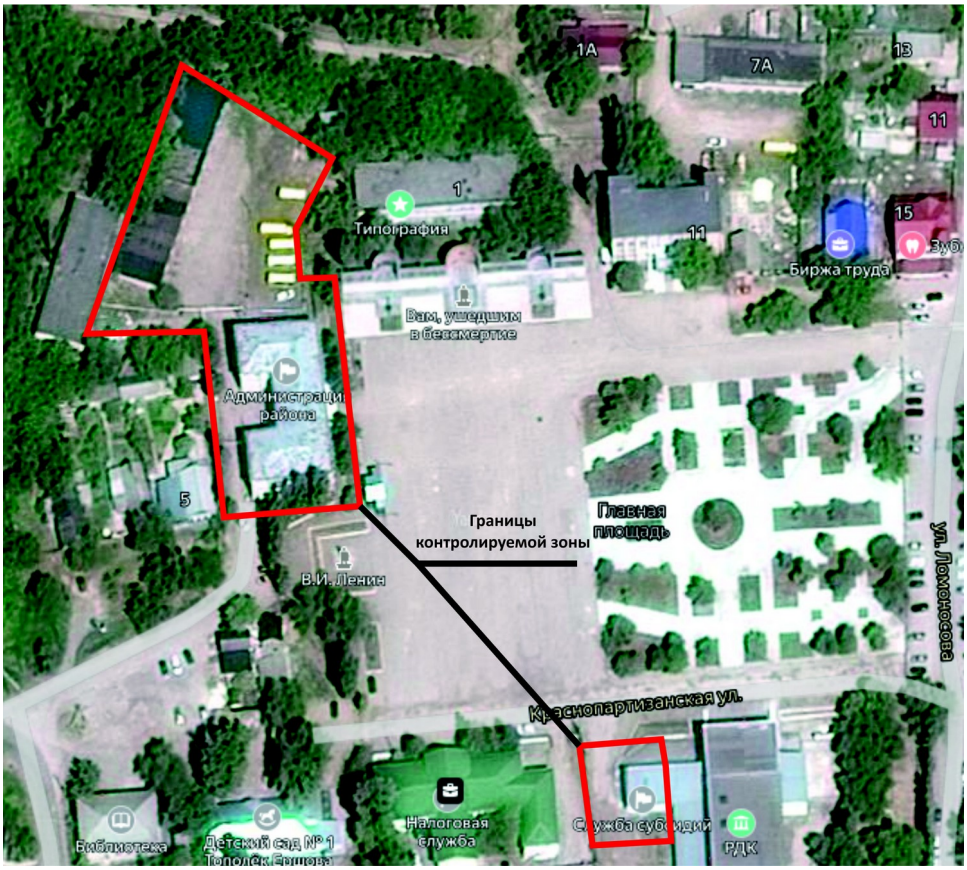
3.1.Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) приведен в Приложении №3.

3.2.Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3.Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение №1 к Положению об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

План-схема
контролируемой зоны помещений по адресу
Саратовская область, г.Ершов, ул.Интернациональная, 7 и ул.Краснопартизанская, 7


1А
7А
13
11
1
Типография
11
15
Биржа труда
Вам, ушедшим в бессмертие
Администрация района
5
Границы контролируемой зоны
Главная площадь
В.И. Ленин
ул. Ломоносова
Красноартизанская ул.
Библиотека
Детский сад № 1
Налоговая служба
РДК