

**АДМИНИСТРАЦИЯ КАИРОВСКОГО СЕЛЬСОВЕТА**

**САРАКТАШСКОГО РАЙОНА ОРЕНБУРГСКОЙ ОБЛАСТИ**

**П О С Т А Н О В Л Е Н И Е**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

14.02.2023 с. Каировка № 11-п

Об утверждении документов в сфере технической защиты информации и персональных данных администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

С целью организации работ по обеспечению безопасности конфиденциальной информации, в том числе персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Указа Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 21 марта 2012 года № 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», руководящих документов Федеральной службы по техническому и экспортному контролю России по технической защите информации:

1. Утвердить:

1.1. Политику информационной безопасности в отношении обработки персональных данных администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №1);

1.2. Положение о порядке организации проведения работ по защите конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №2);

1.3. Правила обработки и обеспечении безопасности персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №3);

1.4. Положение о порядке обработки персональных данных без использования средств автоматизации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №4);

1.5. Руководство пользователя по эксплуатации технических и программных средств защиты конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №5);

1.6. Руководство администратора по эксплуатации технических и программных средств защиты конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №6);

1.7. Руководство пользователя по обеспечению безопасности информационной системы персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №7);

1.8. Руководство администратора по обеспечению безопасности информационной системы персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области а (приложение №8);

1.9. Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации и персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №9);

1.10. Инструкцию пользователя автоматизированной системы в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №10);

1.11. Инструкцию администратора автоматизированной системы по безопасности конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области приложение №11);

1.12. Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №12);

1.13. Перечень сведений конфиденциального характера, подлежащих защите в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение №13);

1.14. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение № 14)

1.15. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение № 15)

1.16. Правила работы с обезличенными персональными данными в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (приложение № 16)

1.17. Положение об обработке персональных данных сотрудников согласно приложению № 17.

2. Распоряжение администрации Каировского сельсовета от 01.07.2013 «Об утверждении документов по защите персональных данных» признать утратившим силу.

3. Постановление вступает в силу после подписания.

4. Контроль за исполнением постановления оставляю за собой.

Глава сельсовета: А.Н.Логвиненко

Разослано: администрации района, прокурору района, в дело

Приложение №1

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

Политика

информационной безопасности в отношении обработки персональных данных администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

1. Общие положения

Политика информационной безопасности (далее – Политика) администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее - администрации), разработана в администрации и является локальным внутренним документом, определяющим основные направления обеспечения безопасности персональных данных и обеспечения безопасности в процессе их обработки.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в концепции информационной безопасности информационных систем персональных данных администрации.

Основными нормативно-правовыми и методическими документами, на которых базируется Политика являются:

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки персональных данных (ПДн), права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
3. Утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Утвержденные Постановлением Правительства Российской Федерации от 06.07.2008 г. № 512 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
5. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства Российской Федерации 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».
7. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15.02.2008.
8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15.02.2008.
9. Приказ 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».

В Политике определены требования к персоналу информационных систем персональных данных (ИСПДн), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн администрации.

Целью настоящей Политики является обеспечение безопасности объектов защиты администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Необходимо осуществлять предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций данных или их уничтожения.

Состав объектов защиты представлен в документах: «Перечень персональных данных, обрабатываемых в администрации, в связи с осуществлением государственных функций», «Перечень персональных данных, обрабатываемых в администрации в связи с реализацией трудовых отношений», «Перечень сведений конфиденциального характера в администрации».

Требования настоящей Политики распространяются на всех сотрудников администрации.

**2. Термины и определения**

В настоящем документе используются следующие термины и 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 её 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;

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

персональные данные **(ПДн)** - 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;

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;

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;

**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).

Применяемые обозначения и сокращения:

АВС – антивирусные средства;

АРМ – автоматизированное рабочее место;

ВТСС – вспомогательные технические средства и системы;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

СОВ – система обнаружения вторжений;

ТКУИ – технические каналы утечки информации;

УБПДн – угрозы безопасности персональных данных.

**3. Система защиты персональных данных**

Система защиты персональных данных (СЗПДн), строится на основании:

Перечня персональных данных, подлежащих защите;

Акта классификации информационной системы персональных данных;

Модели угроз безопасности персональных данных;

Положения о разграничении прав доступа к обрабатываемым персональным данным;

Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн администрации. На основании анализа актуальных угроз безопасности ПДн описанного в модели угроз и отчете о результатах проведения внутренней проверки, дается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Необходимые мероприятия отражены в плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;

- серверы;

- СУБД;

- каналы передачи в сети общего пользования и (или) международного обмена.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн включает следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в список и утверждены главой муниципального образования.

**4. Требования к подсистемам СЗПДн**

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;

- обеспечения целостности и доступности;

- антивирусной защиты;

- межсетевого экранирования;

- анализа защищенности;

- обнаружения вторжений;

- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от требований к определенному уровню защищенности ИСПДн, определенного в Акте классификации информационной системы персональных данных.

4.1. Подсистемы управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

4.2. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн администрации, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

4.3. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн администрации.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

4.4. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- контроля целостности своей программной и информационной части;

- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

- регистрации и учета запрашиваемых сервисов прикладного уровня;

- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратного комплекса межсетевого экранирования.

4.5. Подсистема анализа защищенности обеспечивает выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

4.6. Подсистема обнаружения вторжений обеспечивает выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

4.7. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн администрации, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

**5. Пользователи ИСПДн**

В ИСПДн администрации выделяются следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор АС;

- пользователь АС.

5.1. Администратор АС работник обслуживающей организации по договору, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя к элементам хранящим персональные данные.

Администратор АС обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

- обладает полной информацией о технических средствах и конфигурации ИСПДн;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

5.2. Пользователь АС, сотрудник администрации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь АС не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь АС обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

**6. Требования к персоналу по обеспечению защиты ПДн**

Все сотрудники администрации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника, ответственный сотрудник обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудники администрации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники администрации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники администрации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение на АРМ, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами администрации, третьим лицам.

При работе с ПДн в ИСПДн сотрудники администрации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля (доступом по паролю), если не используются более сильные средства защиты.

Сотрудники администрации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, способных повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн главе муниципального образования.

**7. Должностные обязанности пользователей ИСПДн**

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

* Инструкция по парольной защите в автоматизированной системе администрации;
* Инструкция администратора автоматизированной системы по безопасности конфиденциальной информации в администрации;
* Инструкция по организации антивирусной защиты автоматизированной системы в администрации;
* Инструкция пользователя автоматизированной системы в администрации;
* Должностная инструкция ответственного за организацию обработки персональных данных в администрации;
* Инструкция по обработке персональных данных в администрации, осуществляемой без использования средств автоматизации;
* Обязательство сотрудника администрации, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного контракта прекратить обработку персональных данных, ставших известных ему в связи с исполнением должностных обязанностей;
* Соглашение о неразглашении конфиденциальной информации с сотрудником, доступ которого к конфиденциальной информации, необходим для выполнения им своих трудовых (служебных) обязанностей.

**8. Ответственность пользователей ИСПДн администрации**

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ПК и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ПК или сетей (статьи 272,273 и 274 УК РФ).

Администратор АС несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками администрации – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение №2

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Положение**

**о порядке организации проведения работ по защите конфиденциальной информации в администрации муниципального образования**

**Каировский сельсовет Саракташского района Оренбургской области**

# 1. Общие положения

1.1. Положение о порядке организации проведения работ по защите конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее - Положение) устанавливает порядок организации проведения работ по защите конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – Администрации), определяет виды информационных ресурсов ограниченного доступа компьютерных информационных систем (далее - КИС), а также порядок категорирования этих ресурсов.

1.2. Положение устанавливает основные принципы и организационную структуру системы категорирования информационных ресурсов в администрации, организованных в виде файлов и баз данных, формируемых, накапливаемых и обрабатываемых в КИС, а также в автономных информационных системах, создает необходимые организационно-правовые основания для эффективной защиты конфиденциальной информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите, содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ, применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

1.3. Положение определяет порядок организации доступа пользователей в администрации к информационным ресурсам на основе введения категорий допуска.

1.4. Целью настоящего Положения является:

- укрепление механизмов правового регулирования отношений в области защиты конфиденциальной информации;

- создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

- защита информационных ресурсов от несанкционированного доступа (далее - НСД), обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых.

1.5. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами администрации.

1.6. Настоящее Положение основывается на [Конституции](garantF1://10003000.0) Российской Федерации, [Федеральном законе](garantF1://12048555.0) «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, а также ряде иных нормативных правовых актов в сфере защиты конфиденциальной информации.

1.7. Действие Положения не распространяется на автоматизированные информационные системы хранения и обработки информации, содержащей сведения, составляющие государственную тайну.

1.8. Для оказания услуг в области защиты информации могут привлекаться специализированные организации, имеющие лицензию на данный вид деятельности.

1.9. Используемые технические и программные средства защиты информации должны быть идентифицированы с Постановлением Правительства Российской Федерации от 26 июня 1995 года №608.

1.10. Положение может уточняться и корректироваться по мере необходимости.

# 2. Основные понятия, используемые в настоящем Положении

2.1. В настоящем Положении используются следующие основные понятия:

автоматизированная система (далее - АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

администратор безопасности - ответственное должностное лицо, уполномоченное установленным порядком на проведение работ в области защиты информации и поддержание уровня защиты объекта информатизации и его ресурсов на этапах промышленной эксплуатации данного объекта в установленном штатном режиме работы;

безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т. е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами;

владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах правомочий, установленных законом и/или собственником информации;

доступ к информации (доступ) - 1) получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств; 2) ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации;

доступность информации - состояние информации, характеризуемое способностью АС (приложение 1) обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

**защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

защита от НСД - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил;

защита информации от утечки - деятельность по предотвращению неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к защищаемой информации и получения защищаемой информации (иностранными) разведками;

защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями действующего [законодательства](garantF1://12048555.16);

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

категорирование защищаемой информации (объекта защиты) - установление градаций важности защиты защищаемой информации (объекта защиты);

коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с [законодательством](garantF1://10002673.0) Российской Федерации;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

охраняемые сведения - сведения, составляющие государственную, служебную, коммерческую или личную тайну, на распространение которых накладываются ограничения в установленном порядке, конфиденциальная информация, обрабатываемая с использованием технических средств, сведения конфиденциального характера, содержащиеся в речевой информации;

**пользователь информации** - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

правило доступа к информации (правило доступа) - совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение, пользование и распоряжение указанными объектами;

целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

# 3. Виды угроз информационной безопасности объектов

В качестве угроз информационной безопасности объектов необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения охраняемых сведений, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;

- использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;

- несанкционированный удаленный доступ (из-за пределов контролируемых зон) в сети систем информатизации и связи объектов с целью получения информации ограниченного доступа и использования возможностей систем связи (компьютерная разведка, дистанционный доступ к программным средствам иностранных цифровых электронных автоматических телефонных станций);

- преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты, посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

- непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки проектирования, разработки и эксплуатации технических и программных средств автоматизированных систем.

# 4. Понятие и состав конфиденциальной информации

# 4.1. Состав конфиденциальной информации

4.1.1. Информация в зависимости от категории доступа к ней подразделяется:

- на общедоступную информацию, к которой относятся общеизвестные сведения и иная информация, доступ к которой не ограничен (публикации, сообщения в средствах массовой информации, выступления на конференциях и выставках, интервью и т. п.),

- на информацию, доступ к которой ограничен [федеральными законами](garantF1://12048555.9) (информация ограниченного доступа). Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

4.1.2. Информация ограниченного доступа включает в себя:

- информацию, составляющую государственную тайну (секретную), защита которой осуществляется в соответствии с [законодательством](garantF1://10002673.0) Российской Федерации о государственной тайне;

- конфиденциальную информацию.

4.1.3. К сведениям конфиденциального характера относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных [федеральными законами](garantF1://12048567.0) случаях;

- сведения, составляющие тайну следствия и судопроизводства;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с [Гражданским кодексом](garantF1://10064072.0) Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с [Конституцией](garantF1://10003000.0) Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных сообщений и т. д.);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с [Гражданским кодексом](garantF1://10064072.0) Российской Федерации и [федеральными законами](garantF1://12036454.0) (коммерческая тайна);

- сведения о существе изобретения, полезной модели, промышленного образца до официальной публикации информации о них.

4.1.4. Состав сведений, относящихся к служебной тайне, регламентируется специальным перечнем, который утверждается главой муниципального образования Каировский сельсовет Саракташского района Оренбургской области.

4.1.5. Носители информации, составляющей служебную тайну, могут иметь гриф ограничения доступа «Для служебного пользования». Часто он сопровождается пометами «Лично», «Не для печати», «Не подлежит оглашению», «Только адресату» и др.

4.1.6. Информация ограниченного доступа, не содержащая сведений, отнесенных к государственной тайне, должна иметь гриф конфиденциальности.

4.1.7. При организации защиты конфиденциальных сведений необходимо четко регламентировать:

- перечень сведений конфиденциального характера специалиста по информационным технологиям, осуществляющего техническое обслуживание информационного ресурса администрации;

- процедуру допуска сотрудников к сведениям, составляющим служебную, коммерческую или другую тайну;

- обязанности исполнителей, допущенных к сведениям, которые составляют служебную, коммерческую или другую тайну;

- правила обращения (делопроизводство, учет, хранение, размножение и т.д.) с документами;

- правила доступа (передачи) к информации иных лиц;

- ответственность за разглашение сведений, оставляющих служебную, коммерческую или другую тайну.

# 4.2. Виды конфиденциальной информации в администрации;

# 4.2.1. В автоматизированных системах может обрабатываться информация следующих видов:

- сведения, составляющие государственную тайну;

- сведения, составляющие служебную тайну;

- сведения, составляющие коммерческую тайну;

- персональные данные;

- открытая информация;

- открытая общедоступная информация.

4.2.2. Сведения, составляющие государственную тайну, обрабатываются в автоматизированных системах на базе автономных персональных ЭВМ и в рамках Положения не рассматриваются.

4.2.3. Сведения, составляющие служебную тайну, могут включать служебную предметную информацию и служебную технологическую информацию, представляющую идентификаторы и пароли пользователей, настройки межсетевых экранов и т. д.

4.2.4. Служебная предметная информация, составляющая служебную тайну, должна защищаться в соответствии с требованиями федерального законодательства и РД ФСТЭК «СТР-К».

4.2.5. Служебная технологическая информация, составляющая служебную тайну, должна защищаться в соответствии с требованиями нормативных правовых документов по обеспечению информационной безопасности и защите информации в автоматизированных системах администрации.

4.2.6. Сведения, составляющие коммерческую тайну, могут быть отнесены к сведениям, составляющим служебную тайну с обеспечением их защиты на уровне требований, применяемых к защите служебной тайны, или рассматриваться как коммерческая тайна с обеспечением их защиты на уровне требований [Федерального закона](garantF1://12036454.0) от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».

4.2.7. Обеспечение защиты персональных данных должно обеспечиваться в соответствии с требованиями [Федерального закона](garantF1://12048567.0) от 27 июля 2006г. №152-ФЗ «О персональных данных» и РД ФСТЭК России.

4.2.8. Открытая информация может быть доступна для всех сотрудников органов государственной власти, защите подлежит ее целостность и доступность.

4.2.9. Открытая общедоступная информация размещается на информационных порталах органов государственной власти и издается в публичных изданиях. Защите подлежит ее целостность, доступность и достоверность. Защита этой информации должна обеспечиваться в соответствии с требованиями в объемах законодательства.

4.2.10. Виды информации и требования к защите представлены в следующей таблице:

|  |  |  |  |
| --- | --- | --- | --- |
| Вид информации | Конфиденциальность | Целостность | Доступность |
| Сведения, составляющие государственную тайну | + | + | + |
| Сведения, составляющие служебную тайну | + | + | + |
| Сведения, составляющие коммерческую тайну | + | + | + |
| Сведения, составляющие служебную тайну (технологическая информация) | + | + |  |
| Персональные данные | + | + | + |
| Открытая информация | - | + | + |
| Открытая общедоступная информация | - | + | + |

4.2.11. Любая информация ограниченного доступа, вне зависимости от форм хранения, подлежит адекватной (дифференцированной) защите, в том числе:

- речевая информация;

- информация, циркулирующая в средствах связи и вычислительной техники;

- информация, передаваемая по каналам связи, локальным или глобальным вычислительным сетям;

- информация, представленная в виде информативных акустических и - электромагнитных сигналов, физических полей;

- информация на бумажной, магнитной или другой основе;

- информационные массивы и базы данных, которые должны защищаться в соответствии с законодательством Российской Федерации.

4.2.12. К сведениям, подлежащим защите в администрации, относятся:

- сведения, определенные Перечнем сведений конфиденциального характера соответствующего специалиста по информатизации, осуществляющего техническое обслуживание информационного ресурса администрации, утверждаемых главой муниципального образования Каировский сельсовет Саракташского района Оренбургской области;

- иные сведения, составляющие охраняемую действующим законодательством тайну;

- иные сведения, определенные собственником информации (федеральные органы исполнительной власти, их территориальные органы) при ее передаче администрации в соответствии с соглашениями о конфиденциальности в рамках их совместной деятельности.

4.2.13. Перечень сведений специалиста, осуществляющего техническое обслуживание информационного ресурса администрации, составляющих служебную и коммерческую тайну, утверждается главой муниципального образования Каировский сельсовет Саракташского района Оренбургской области и определяет сведения, которые не подлежат разглашению в открытой переписке, переговорах по открытым каналам связи и в средствах массовой информации. Перечень охватывает информацию ограниченного распространения по всем сферам деятельности администрации.

4.2.14. Перечень разрабатывается в соответствии с [Федеральным законом](garantF1://12048555.0) от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», [Указом](garantF1://10100083.0) Президента Российской Федерации от 6 марта 1997г. №188 «Об утверждении перечня сведений конфиденциального характера», [постановлением](garantF1://10005921.0) Правительства Российской Федерации от 5 декабря 1991г. №35 «О перечне сведений, которые не могут составлять коммерческую тайну», [постановлением](garantF1://88429.0) Правительства Российской Федерации от 3 ноября 1994г. №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» и другими правовыми актами, определяющими состав сведений ограниченного распространения.

# 5. Информационные ресурсы ограниченного доступа компьютерной информационной системы администрации

5.1. К информационно-телекоммуникационным системам конфиденциального характера в контексте необходимости их защиты относятся:

- информационные ресурсы администрации (файлы, базы данных, электронные и бумажные документы и т. д.), подлежащие защите;

- системы формирования, обработки, распространения и использования информационных ресурсов;

- информационная инфраструктура автоматизированных систем администрации.

5.2. Система формирования, обработки, распространения и использования информационных ресурсов включает в себя:

- информационные подсистемы автоматизированных систем администрации, библиотеки, архивы, базы и банки данных;

- информационные технологии, регламенты и процедуры сбора, обработки, хранения, преобразования и отображения информации, а также специальные средства их своевременного уничтожения;

- нормативно-правовые положения, определяющие функции, права и ответственность участников данной системы;

- персонал, занятый в данной системе.

5.3. Информационная инфраструктура включает в себя:

- сеть передачи данных администрации в центры обработки и анализа информации;

- каналы связи, информационного обмена и телекоммуникации;

- механизмы обеспечения работоспособности телекоммуникационных систем и сетей;

- системы и средства защиты информации;

- системы документационного обеспечения управления, мониторинга и прогнозирования.

5.4. Объектами защиты в автоматизированных системах администрации являются:

- информация (в любой форме ее представления), содержащая охраняемые сведения;

- информационные системы, включая системы связи;

- технические средства связи и информатизации (средства вычислительной техники, информационно-вычислительные комплексы, средства и системы связи, передачи данных, телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов, другие технические средства обработки информации), используемые для обработки, хранения и передачи информации, содержащей охраняемые сведения;

- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программно-математическое обеспечение), используемые для обработки информации, содержащей охраняемые сведения;

- документация на технические и программные средства связи и информатизации, используемые в обработке, хранении и передаче информации, содержащей охраняемые сведения;

- технические средства, не используемые в обработке, хранении и передаче конфиденциальной информации, но расположенные в помещениях, где обрабатывается (циркулирует) информация, содержащая охраняемые сведения;

- программные средства, не обрабатывающие информацию ограниченного доступа, но размещенные на объектах связи и информатизации, обрабатывающих, хранящих и передающих информацию, содержащую охраняемые сведения;

- помещения, предназначенные для обработки и хранения информации, содержащей охраняемые сведения.

# 6. Информационные ресурсы, подлежащие защите

6.1. Информационные ресурсы, содержащие или обрабатывающие сведения конфиденциального характера, определяются Перечнем информационных ресурсов администрации, в соответствии с Перечнем сведений конфиденциального характера.

6.2. Этот перечень должен включать названия информационных систем (подсистем), автоматизированных рабочих мест, баз данных и пакетов прикладных программ, подлежащих защите.

6.3. Перечень информационных ресурсов администрации, содержащих сведения конфиденциального характера, утверждается главой муниципального образования Каировский сельсовет Саракташского района.

# 7. Категории конфиденциальных информационных ресурсов

7.1. В целях формирования дифференцированного подхода к обеспечению защиты информационных ресурсов автоматизированных систем администрации осуществляется инвентаризация и категорирование информационных ресурсов.

7.2. Инвентаризация предполагает проведение паспортизации и учета всех информационных ресурсов администрации.

7.3. Под категорированием информационного ресурса понимается комплекс организационно-технических мероприятий по отнесению информационного ресурса к соответствующей категории, характеризующей важность сохранения его функционирования, а также обеспечения целостности и конфиденциальности, содержащейся в нем информации. Обязательному категорированию подлежат как находящиеся в эксплуатации, так и вновь вводимые в эксплуатацию информационные ресурсы администрации.

7.4. Для информационных ресурсов администрации муниципального образования Каировский сельсовет Саракташского района установлены следующие категории:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Категория | Гриф | Требования к защите | Характер информации | Группы пользователей |
| 1 | 2 | 3 | 4 | 5 |
| I категория | Строго конфиденциально | Высокие требования к обеспечению конфиденциальности, целостности и доступности информационных ресурсов | Важная плановая, производственная и коммерческая информация | Высший руководящий состав |
| II категория | Конфиденциально | Средние требования к обеспечению конфиденциальности. Требования к целостности и доступности определяются в зависимости от конкретных требований к информационному ресурсу | Коммерческая информация | Сотрудники администрации в части, касающейся их информации |
| III категория | ДСП | Низкие требования к обеспечению конфиденциальности. Требования к целостности и доступности определяются в зависимости от конкретных требований к информационному ресурсу | Общая нормативная, коммерческая и другая информация для служебного пользования | сотрудники администрации |
| Технологическая категория | Т  (ДСП-Т) | Высокие требования к обеспечению конфиденциальности, целостности и доступности информационных ресурсов | Технологическая информация и информация системы защиты (пароли, идентификаторы, IP-адреса, классификаторы и т. д.) | Администратор систем |

7.5. Основные требования по обеспечению конфиденциальности, целостности и доступности для конкретных информационных ресурсов определяются на этапе их проектирования, создания и ввода в эксплуатацию.

7.6. Специальные требования к защищенности информационного ресурса определяются администратором систем при участии владельца информационного ресурса на этапе их ввода в эксплуатацию.

7.7. Для каждой из категорий устанавливается:

- порядок назначения и изменения необходимых полномочий пользователей по доступу к информационным ресурсам категории;

- порядок эксплуатации оборудования и программного обеспечения, используемого для работы с информационными ресурсами категории;

- порядок обеспечения конфиденциальности, целостности и доступности информационных ресурсов категории;

- порядок принятия ответных мер в случае выявления действий, направленных на нарушение конфиденциальности, целостности или доступности информационных ресурсов категории.

**8. Организационная структура системы присвоения категории информационным ресурсам**

8.1. Организационную структуру системы присвоения категорий информационным ресурсам образуют:

Специалист по защите информации администрации, осуществляющий организацию эксплуатации информационного ресурса;

# 9. Порядок присвоения категорий информационным ресурсам

9.1. Подготовка информационного ресурса к категорированию предполагает его инвентаризацию и информационное обследование.

9.2. Инициатором категорирования информационного ресурса должен выступать его владелец, который подает заявку в Комиссию.

9.3. Для проведения технических работ по инвентаризации и категорированию информационного ресурса Комиссия создает рабочую группу в составе специалистов - владельца информационного ресурса и администратора систем администрации.

9.4. По результатам инвентаризации и информационного обследования составляется формуляр информационного ресурса, отражающий основные характеристики информационного ресурса.

9.5. Ответственность за составление и поддержание в актуальном состоянии формуляров информационных ресурсов автоматизированных систем администрации возлагается на администратора систем, осуществляющего техническое обслуживание информационного ресурса, отвечающего за защиту конфиденциальной информации.

9.6. В процессе эксплуатации информационного ресурса все изменения характеристик информационного ресурса, зафиксированных в формуляре информационного ресурса, доводятся владельцем информационного ресурса до сведения главы муниципального образования Каировский сельсовет Саракташского района.

9.7. При недостаточности или неточности исходных данных составление формуляра информационного ресурса производится на основании результатов комплексных испытаний информационного ресурса и имеющихся средств защиты в реальных условиях эксплуатации, а также анализа структуры информационного ресурса, технических средств, программного обеспечения и технической документации.

9.8. На основании данных произведенного информационного обследования и документирования информационного ресурса, специалист по защите информации вносит предложение о присвоении категории информационному ресурсу на рассмотрение главе муниципального образования Каировский сельсовет Саракташского района.

9.9. Информационные ресурсы, содержащие конфиденциальную информацию, вносятся в установленном порядке в перечень информационных ресурсов администрации, содержащих сведения конфиденциального характера.

# Глава 10. Доступ к информационным ресурсам

# 10.1. Порядок организации доступа к информационным ресурсам администрации:

10.1.1. Порядок организации доступа к информационным ресурсам автоматизированных систем администрации включает:

- разделение пользователей автоматизированных систем на категории пользователей в соответствии с предоставляемыми им возможностями по обработке категорированной информации;

- подготовку заявки на разрешение доступа сотрудника администрации к конкретным информационным ресурсам;

- визирование заявки владельцем информационного ресурса, специалистом по защите информации администрации, и подготовка распоряжения администратору информационного ресурса о регистрации нового пользователя с назначенными ему полномочиями;

- выполнение администратором информационного ресурса необходимых технических действий по регистрации нового пользователя.

# 10.2. Порядок оформления права на доступ к информационным ресурсам

10.2.1. Доступ конкретного пользователя к конкретному информационному ресурсу осуществляется на основании заявки, которую подает специалист по информационным технологиям, осуществляющий техническое обслуживание информационного ресурса администрации.

10.2.2. В заявке указываются должность и фамилия сотрудника, перечень информационных ресурсов, необходимых для исполнения должностных обязанностей, полномочия сотрудника по их обработке, интервалы разрешенного времени работы сотрудника с информационными ресурсами.

10.2.3. Заявка передается владельцу информационного ресурса в установленном порядке.

10.2.4. Специалист по информационным технологиям, осуществляющий техническое обслуживание информационного ресурса осуществляет ознакомление пользователя с правилами эксплуатации конкретного ресурса и требованиями по обеспечению информационной безопасности при работе с ним. Им также предоставляется право проверки знания пользователем установленных правил и требований работы с информационным ресурсом и допуска к работе с ним.

10.2.5. При готовности пользователя к работе с информационным ресурсом готовится распоряжение администратору информационного ресурса о регистрации указанного пользователя для работы с ним.

10.2.6. Регистрация нового пользователя осуществляется специалистом по информационным технологиям, осуществляющего техническое обслуживание информационного ресурса на основании зарегистрированного в журнале учета распоряжения, полученного от руководителя администрации.

10.2.7. После выполнения технических работ по проведению регистрации нового пользователя администратор информационного ресурса сообщает ему о возможности начала работы с информационным ресурсом.

10.2.8. Администратор информационного ресурса не имеет права включать, удалять и модифицировать регистрационные параметры пользователей без соответствующих зарегистрированных распоряжений своего руководителя.

# 11. Разделение пользователей автоматизированных систем на категории пользователей

11.1. Для обеспечения разграничения доступа пользователей автоматизированных систем администрации к категорированной информации вводятся следующие категории пользователей:

|  |  |  |
| --- | --- | --- |
| Категории пользователей | Группы  пользователей | Категории ин формации,  к которым разрешен доступ |
| I категория | Высший руководящий состав | I, II, III и общая категории |
| II категория | Руководители и сотрудники, имеющие допуск к информации II категории в части, касающейся | II, III и общая категории |
| III категория | Руководители и сотрудники администрации | III и общая категории |
| Технологическая категория (Т) | Администраторы систем | Технологическая, III и общая категории |
| Общая категория | Сотрудники администрации, жители поселка. Пользователи открытых сетей | Общая категория |

11.2. Для введенных категорий пользователей автоматизированных систем администрации разрешен доступ к информационным ресурсам, категории которых перечислены в третьем столбце таблицы, если не оговорены другие условия.

11.3. Категорирование пользователей осуществляется в соответствии с категорией, занимаемой ими должности, характеристики которой приведены во втором столбце таблицы.

11.4. При необходимости предоставления доступа пользователю определенной категории к информационному ресурсу, принадлежащему к более высокой категории, разрешение на этот доступ получается в индивидуальном порядке по согласованной договоренности сторон.

# 12. Ответственность за нарушение режима конфиденциальности

12.1. Нарушением режима конфиденциальности в отношении перечисленных информационных систем администрации является разглашение служебной или коммерческой тайны, которое влечет ответственность в соответствии с действующим [законодательством](garantF1://12036454.0) Российской Федерации.

12.2. Ответственность за нарушение требований обеспечения информационной безопасности накладывается на должностных лиц и сотрудников администрации и зависит от величины причиненного ущерба. Сотрудники администрации могут привлекаться к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством.

12.3. Ответственность за обеспечение защиты информации ограниченного доступа несут владельцы информационных ресурсов.

Приложение 1

к [Положению](#sub_1000) о порядке организации

проведения работ по защите

конфиденциальной информации в администрации

муниципального образования

Каировский сельсовет

Саракташского района

Оренбургской области

# Список сокращений

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| БД | База данных |
| ВТСС | Вспомогательные технические средства и системы |
| ИР | Информационные ресурсы |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| КИС | Компьютерная информационная система |
| ЛВС | Локальная вычислительная сеть |
| МЭ | Межсетевой экран |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ОТСС | Основные технические средства и системы |
| ПО | Программное обеспечение |
| ПЭМИН | Побочные электромагнитные излучения и наводки |
| РД | Руководящий документ |
| СВТ | Средства вычислительной техники |
| СЗИ | Система защиты информации |
| СКЗИ | Средства криптографической защиты информации |
| СТР | РД ФСТЭК России "Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)" |
| СТР-К | РД ФСТЭК России "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)" |
| СУБД | Система управления базами данных |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю Российской Федерации (Гостехкомиссия России) |
| [ЭЦП](garantF1://84059.32) | Электронная цифровая подпись |
| ПЭВМ | Персональная электронная вычислительная машина |
| ЭВМ | Электронная вычислительная машина |
| ДСП | Для служебного пользования |
| ДСП-Т | Для служебного пользования (технологическая) |

Приложение №3

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Правила**

**обработки и обеспечении безопасности персональных данных в администрации муниципального образования**

**Каировский сельсовет Саракташского района Оренбургской области**

1. Настоящие Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в администрации Каировского сельсовета Саракташского района Оренбургской области (далее - администрации) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 года № 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 Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2. Настоящие Правила устанавливают единый порядок действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными в администрации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в администрации.

3. Целью настоящих Правил является обеспечение защиты прав и свобод при обработке персональных данных работников администрации, а также граждан, обратившихся в администрацию (далее – субъект персональных данных), установление ответственных должностных лиц, имеющих доступ к персональным данным, ответственности за невыполнение норм, регулирующих обработку и защиту персональных данных.

4. В настоящих Правилах используются основные понятия, установленные статьей 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ).

5. Ответственные должностные лица администрации, в должностные обязанности которых входит осуществление обработки персональных данных либо осуществление доступа к персональным данным (далее – ответственные лица) определяются распоряжением руководителя (работодателя), в обязательном порядке знакомятся под роспись с постановлением администрации, утверждающим перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», а также подписывают обязательство о неразглашении персональных данных по форме согласно приложению к настоящим Правилам.

6. Обработка персональных данных в администрации осуществляется на основе принципов, установленных [статьей 5](consultantplus://offline/ref=53B3D53B6438C04BFA75C8165EA71635E8D85C41949FE8935451689C2F14A4A72DC490D2DD852E7EG1Q9D) Федерального закона № 152-ФЗ.

7. Обработка персональных данных субъекта персональных данных осуществляется после:

1) получения письменного согласия субъекта персональных данных или его представителя на обработку персональных данных, за исключением случаев, предусмотренных [частью 2 статьи 6](garantf1://12048567.602/) Федерального закона № 152-ФЗ. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления муниципальных услуг, устанавливается Правительством Российской Федерации.

2) направления до начала обработки персональных данных уведомления в Управление федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Оренбургской области о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 [статьи](consultantplus://offline/ref=C8423A9083AB97EA2CDE7822F9F33F00792F79A33C377913796D3719E8911B0D251E6728F276D866m2HBD) 22 Федерального закона № 152-ФЗ;

3) принятия необходимых мер по обеспечению безопасности персональных данных.

8. При обработке персональных данных ответственные лица обязаны соблюдать следующие требования:

1) обработка персональных данных осуществляется в целях обеспечения соблюдения [Конституции](consultantplus://offline/ref=B9CC44F336E343E3DEC368B7E9816189CE28A3D132F81C790F3897R4V6C) Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия в трудоустройстве, обучении и должностном росте, обеспечения личной безопасности работников администрации и членов их семей, а также в целях обеспечения сохранности принадлежащего им имущества и имущества администрации;

2) персональные данные следует получать лично у субъекта персональных данных, в случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом субъекта персональных данных заранее, получить его письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных;

3) запрещается получать, обрабатывать и приобщать к личному делу субъекта персональных данных не установленные Федеральными законами [№ 79-ФЗ](consultantplus://offline/ref=B9CC44F336E343E3DEC368B7E9816189CD22A6D43AA74B7B5E6D9943C9REVFC) и [№ 152-ФЗ](consultantplus://offline/ref=B9CC44F336E343E3DEC368B7E9816189CD21A3D131A94B7B5E6D9943C9REVFC) персональные данные об их политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

4) при принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

5) защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств администрации в порядке, установленном Федеральным [законом](consultantplus://offline/ref=B9CC44F336E343E3DEC368B7E9816189CD21A3D131A94B7B5E6D9943C9REVFC) № 152-ФЗ и иными нормативными правовыми актами.

9. При передаче персональных данных ответственные лица администрации обязаны соблюдать следующие требования:

1) не сообщать персональные данные субъекта персональных данных без его письменного согласия для использования их в коммерческих целях;

2) предупреждать лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные должны использоваться только в целях, для которых они сообщены, и требовать от этих лиц подтверждения о соблюдении требований;

3) передавать персональные данные субъекта персональных данных его представителю в порядке, установленном федеральными законами, и ограничивать эту информацию только теми персональными данными субъекта персональных данных, которые необходимы для выполнения представителем его функций.

10. Передача персональных данных от администрации иному оператору персональных данных допускается в минимальных объемах, в целях выполнения задач, соответствующих объективной причине сбора этих данных, и только после заключения с этим оператором договора о соблюдении конфиденциальности.

11. Не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону или факсу.

12. Персональные данные и иные сведения, содержащиеся в личных делах работников администрации, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

13.Ответственные лица администрации при обработке персональных данных с использованием информационных систем обязаны:

- принимать меры, исключающие несанкционированный доступ к используемым программно-техническим средствам;

- вести учет электронных носителей информации (включая резервные и архивные копии), осуществлять хранение документов, содержащих персональные данные, и электронных носителей информации в металлических шкафах или сейфах;

- производить запись персональных данных (отдельных файлов, баз данных) на электронные носители только в случаях, регламентированных порядком работы с данными сведениями;

- соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей;

- принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам;

- работать с информационными системами в объеме своих полномочий, не допускать их превышения;

- обладать навыками работы с антивирусными программами в объеме, необходимом для выполнения функциональных обязанностей и требований по защите информации.

14. При работе на персональном компьютере, в том числе для доступа к информационным системам, запрещается:

- записывать значения кодов и паролей доступа;

- передавать коды и пароли доступа другим лицам;

- пользоваться в работе чужими кодами и паролями доступа;

- производить подбор кодов и паролей доступа других пользователей;

- записывать на электронные носители с персональными данными посторонние программы и данные;

- копировать данные на неучтенные электронные носители информации;

- выносить электронные носители с персональными данными за пределы организации без согласования с руководителем организации;

- покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств, блокирования доступа к персональному компьютеру;

- приносить, самостоятельно устанавливать и эксплуатировать на технических средствах любые программные продукты, не принятые к эксплуатации;

- открывать, разбирать, ремонтировать технические средства, вносить изменения в конструкцию, подключать нештатные блоки и устройства;

- передавать технические средства для ремонта и обслуживания сторонним организациям без извлечения носителей, содержащих персональные данные.

15. Обработка персональных данных субъекта в информационных системах администрации с использованием средств автоматизации осуществляется в соответствии с Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

16. Защита персональных данных работников в администрации обеспечивается мерами, включающими в себя охрану помещений, в которых ведется обработка персональных данных, содержащихся в личных делах, а также в электронном виде в информационных системах, контроль за соблюдением установленных требований, обеспечение режима безопасности в этих помещениях, обеспечение сохранности носителей персональных данных и средств их защиты, исключение несанкционированного проникновения или пребывания в этих помещениях посторонних лиц, контроль за эффективностью предусмотренных мер защиты.

17. Все документы, компакт-диски, флеш-накопители, содержащие персональные данные, подлежат уничтожению на основании актов только с применением соответствующих уничтожителей.

18. Администрация при обработке персональных данных в информационных системах персональных данных обеспечивает:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) недопущение воздействий на технические средства автоматизированной обработки персональных данных, в результате которых, нарушается их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности персональных данных.

19. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

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

2) охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных;

3) документа, подтверждающего эффективность применяемых мер и средств защиты по нейтрализации актуальных угроз безопасности, определенных в частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

4) утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации информационных систем персональных данных, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и методических документов.

20. Обработка и защита персональных данных в информационных системах персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) осуществляется в соответствии с [Положени](consultantplus://offline/ref=53B3D53B6438C04BFA75C8165EA71635E1D95B469493B5995C08649E281BFBB02A8D9CD3DD852DG7QAD)ем об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

21. Неавтоматизированная обработка персональных данных осуществляется на бумажных носителях в виде документов и в электронном виде (файлы, базы данных) на электронных носителях информации.

22. При неавтоматизированной обработке персональных данных:

1) не допускается фиксация на одном бумажном носителе персональных данных, цели обработки, которых заведомо не совместимы;

2) персональные данные обособляются от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

3) документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

4) дела с документами, содержащими персональные данные, имеют внутренние описи документов с указанием цели обработки и категории персональных данных.

23. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

24. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, со сроком хранения.

25. Личные дела хранятся в помещении администрации, доступ в которое ограничен. Уборка помещения производится только в присутствии работников.

26. Личные дела уволенных работников администрации хранятся в течение 10 лет со дня увольнения, после чего передаются на хранение в муниципальный архив.

27. Сотрудники администрации, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №4

к постановлению

Администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Положение**

о порядке обработки персональных данных без использования средств автоматизации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

**1. Общие положения**

1.1. Настоящее Положение о порядке обработки персональных данных без использования средств автоматизации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и устанавливает единый порядок обработки персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – администрации).

1.2. Используются следующие термины и понятия:

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

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

3) 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;

4) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

5) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

7) 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;

8) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

9) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Задачи, решаемые в процессе обработки персональных данных:

- документационное обеспечение обработки персональных данных;

- защита документированной информации, содержащей персональные данные.

**2. Основные условия проведения обработки персональных данных**

1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных ст.6 ч.1 п.2-11 Федерального закона «О персональных данных»;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Оренбургской области;

- после принятия необходимых мер по защите персональных данных.

В администрации распоряжением главы муниципального образования назначается сотрудник, ответственный за защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

1. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные.
2. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.

**3. Система доступа к конфиденциальным документам**

* 1. Система доступа представляет собой совокупность норм и правил, определяющих, кто из руководителей администрации, кому из пользователей и с какими категориями документов может давать разрешение на ознакомление
  2. Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться сотрудникам, письменно оформившим с организацией отношения о неразглашении, ставших им известными конфиденциальных сведений. Письменное оформление отношений о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа исполнителей к документам;

- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного исполнителя;

- система доступа должна давать возможность обеспечивать исполнителей всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностное лицо. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления исполнителя только с частью документа в разрешении на ознакомление должны быть указаны разделы (пункты или страницы), с которыми можно ознакомить исполнителя.

Доступ сотрудников администрации к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом необходимо выполнить следующие условия:

- ознакомить работника под роспись с перечнем конфиденциальной информации;

- ознакомить работника под роспись с установленным в администрации режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создать работнику необходимые условия для соблюдения им установленного режима по охране конфиденциальности.

3.4. Допуск сотрудников к персональным данным осуществляется приказом главы муниципального образования.

3.5. Со стороны сотрудника администрации предполагается принятие следующих обязательств:

- по соблюдению установленного в администрации режима по охране конфиденциальности;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в специальном соглашении или в течение трех лет, если такое соглашение на заключалось, и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);

- о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации.

1. **Порядок обработки персональных данных без использования средств автоматизации**
   1. Порядок обработки персональных данных на бумажном носителе.

4.1.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных и магнитных носителях.

* + 1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
    2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

* + 1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.2. Порядок обработки персональных данных в электронном виде без использования средств автоматизации.

* + 1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.
    2. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

**5. Подготовка и учет документов, содержащих персональные данные**

* 1. Бланки типовых форм документов (справки, карточки, талоны, ведомости и т.п.) могут изготавливаться при помощи средств вычислительной техники или на пишущей машинке. После изготовления указанные бланки подлежат предварительному учету.
  2. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, на пишущей машинке или рукописным способом.
  3. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера. Учетный номер проставляется на каждом листе документа (если документ подготовлен на двух и более листах).
  4. Для каждого вида документов заводятся свои журналы учета.

**6. Получение (отправление) документов и их учет**

6.1. Все документы, поступающие из других организаций, подлежат регистрации по журналу учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется запись о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления, количество листов.

6.2. При наличии приложений, кроме отметки о поступлении документа, на первом листе каждого приложения в правом нижнем углу проставляется запись «К вх. №\_\_\_» с указанием номера, присвоенного документу в целом.

6.3. Поступившие документы должны обрабатываться и передаваться на рассмотрение руководству администрации в день их получения и оперативно доводиться до исполнителей.

6.4. Отправление документов в другие организации производится в конвертах (пакетах). Конверты (пакеты), в которых отправляются документы, должны быть светонепроницаемыми или иметь вкладки из светонепроницаемой бумаги.

6.5. Пересылка документов может осуществляться через органы фельдъегерской, специальной связи или через почтовое отделение связи.

6.6. Об отправленных документах производятся соответствующие отметки в учетных формах.

**7. Учет документов выделенного хранения**

7.1. Учет документов выделенного хранения охватывает все документы, не подлежащие подшивке в дела. К таким документам относятся:

- документы, которые по производственным условиям нецелесообразно подшивать в дела (различного рода инструкции, положения, справочники, каталоги и т.п.);

- документы, которые по их внешним особенностям невозможно или нецелесообразно подшивать в дела (большого формата, сброшюрованные, чертежно-графические и т.п.);

- рабочие тетради исполнителей (пользователей).

7.2. На учет выделенного хранения документы ставятся непосредственно при их получении или создании, а также при переводе с других видов учета (при необходимости).

7.3. Учет документов, подлежащих выделенному хранению, осуществляется по отдельным журналам.

7.4. Журналы учета документов выделенного хранения ведутся непрерывно. Номера каждого года продолжают номера предыдущих лет.

**8. Копирование документов**

При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.

На некоторых документах может стоять запись о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.

Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители подразделений), наделенные правом распоряжения сведениями.

Документы, поступившие из других организаций, должны копироваться с письменного разрешения руководителя организации или с письменного разрешения издавших их организаций.

Разрешение на изготовление дополнительных экземпляров (копий) учтенного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.

Подлежащие копированию документы регистрируются в журнале учета копирования документов.

На копиях экземпляров документа проставляются их номера. При этом номера копий продолжают номера ранее изготовленных экземпляров.

**9. Формирование дел**

Для обеспечения быстрого поиска необходимых документов, создания условий для их сохранности и удобства пользования, исполненные документы, зарегистрированные по журналам учета поступивших и изданных документов, должны быть сгруппированы в дела. Дело представляет собой совокупность документов, относящихся к одному вопросу или направлению деятельности и помещенных в отдельную обложку.

Распределение документов по делам производится в течение года по мере исполнения документов в соответствии с номенклатурой дел.

Номенклатура дел – это оформленный в установленном порядке систематизированный перечень наименований заводимых дел, с указанием их условных номеров (индексов), сроков хранения и лиц, которым предоставлено право пользования конкретными делами.

Номенклатура дел организации разрабатывается на каждый год, подписывается сотрудником, определенным в п. 2.2., утверждается руководителем организации.

Непосредственное формирование дел включает в себя распределение документов по делам в соответствии с номенклатурой и систематизацию документов внутри дел. Дела формируются в течение года по мере поступления в них документов.

В дела помещаются исполненные документы, оформленные в установленном порядке.

В деле группируются, как правило, документы одного календарного года. При необходимости, по отдельным вопросам допускается ведение переходящих дел.

Внутри дел документы систематизируются в основном в хронологической последовательности.

Каждое дело должно содержать не более 250 листов. При большем количестве листов заводятся в последовательности тома дела, которые должны иметь один и тот же индекс (номер) и заголовок.

Формирование дел производится путем подшивки документов в обложки. Дела постоянного и долговременного сроков хранения должны иметь твердые обложки.

После подшивки документа в дело в журнале учета проставляются индекс (номер) дела, его том и номера листов дела (тома).

При заведении дела в него подшивается необходимое количество листов внутренней описи документов дела. Данные о документах вносятся в опись в момент подшивки документов.

Листы дела нумеруются. Нумерация производится при подшивке документа арабскими цифрами простым графитовым карандашом в правом верхнем углу листа без затрагивания текста документа. Если дело имеет несколько томов, нумерация листов производится по каждому тому отдельно.

Листы внутренней описи документов дела нумеруются отдельно римскими цифрами.

Листы каждого тома дела при закрытии проверяются, прошиваются плотной ниткой в четыре прокола и опечатываются бумажной наклейкой из папиросной или другой тонкой, но не расслаивающейся бумаги (например, калька) с оттиском печати делопроизводства.

**10. Подготовка дел и документов для архивного хранения или уничтожения**

10.1. По истечении определенного времени дела и документы, содержащие конфиденциальную информацию должны передаваться для архивного хранения.

10.2. Дела и документы, утратившие свое практическое значение, подлежат уничтожению.

10.3. Состав государственных и муниципальных органов власти и подведомственных им предприятий, передающих документы постоянного хранения в государственные архивы, а также категории передаваемых ими документов (все документы постоянного хранения или часть из них), определяются Федеральным архивным агентством и органами управления архивным делом субъектов Российской Федерации. В отношении негосударственных предприятий такое определение производится архивными учреждениями совместно с собственниками документов и оформляется договором.

10.4. Документы, подлежащие передаче в государственные архивы, до их фактической передачи должны храниться соответствующим образом оформленными в архиве.

10.5. В таком же порядке хранятся до их уничтожения и документы, не подлежащие передаче в государственные архивы.

10.6. С целью уточнения или определения сроков хранения документов и их отбора для архивного хранения или уничтожения проводится экспертиза ценности документов. Проведение такой экспертизы возлагается на экспертную комиссию.

10.7. Экспертиза ценности дел и документов проводится не реже одного раза в год.

10.8. При определении или уточнении сроков хранения документов необходимо руководствоваться «Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения».

* 1. Если в администрации имеются документы, не предусмотренные названным Перечнем, то срок их хранения следует устанавливать на основе определенных критериев оценки документов, к важнейшим из которых относятся:

- содержание документа (значимость отображенного события, полнота его освещения, новизна, уникальность информации или ее повторяемость, целевое назначение документа);

- происхождение документа (место и время издания);

- внешние особенности документа (подлинник или копия, характер резолюций, физическое состояние).

10.10. После завершения работы по отбору дел и документов для архивного хранения, проводится работа по отбору дел и документов для уничтожения.

10.11. Уничтожение дел и документов производится по акту комиссией в составе не менее 3-х человек, назначаемой приказом главы администрации муниципального образования. Уничтожение должно производиться путем сжигания или с помощью бумагорезательных машин.

**11. Режим сохранности документов**

* 1. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.
  2. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.
  3. В целях обеспечения дополнительных гарантий от проникновения посторонних лиц указанные помещения (по возможности) должны располагаться на средних этажах зданий, а их окна – выходить на внутреннюю территорию объекта.
  4. Право входа в такие помещения имеют глава муниципального образования и сотрудники, имеющие прямое отношение к обработке и хранению документов.

**12. Контроль наличия документов**

12.1. Цель проверок состоит в обеспечении контроля за сохранностью документов. Это достигается путем установления фактического наличия документов учетным данным, выявления отсутствующих документов и принятия мер по их поиску.

12.2. Проверки наличия документов производятся, как правило, один раз в год, по окончании календарного года (годовая проверка). Проверке подлежат все виды документов, независимо от времени их изготовления (поступления).

12.3. Проверка проводится комиссией в составе не менее 3-х человек, назначаемой распоряжением главы муниципального образования.

12.4 В ходе проверки комиссией проводится сверка регистрационных данных и фактического наличия документов, а также выверяется движение (поступление, отправка, размножение, уничтожение) документов в истекшем году.

12.5. По результатам проверки составляется акт, в котором указываются:

- состав комиссии и срок проведения проверки;

- основание для проведения проверки;

- общее количество взятых на учет документов за проверяемый период по всем видам документов раздельно;

- количество и регистрационные номера документов, не предъявленных в ходе проверки, причины их отсутствия;

- факты выявления неучтенных документов, причины данных фактов;

- выявленные нарушения в учете и хранении документов;

- выводы и предложения по результатам проверки.

Акт проверки подписывается всеми членами комиссии и утверждается руководителем организации.

12.6. Внеплановые проверки наличия документов проводятся:

- при смене сотрудников, ответственных за документы;

- при временном отсутствии сотрудников (убытии в отпуск, командировку, по болезни);

- по решению руководителя организации (полугодовая, квартальная).

Приложение №5

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Руководство**

пользователя по эксплуатации технических и программных средств защиты конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

## 1. Общие положения

1.1. Пользователем является каждый сотрудник администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – администрации), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки конфиденциальной информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.2. Пользователь несет персональную ответственность за свои действия.

1.3. Пользователь в своей работе использует настоящее руководство, [Политику информационной безопасности](file:///D:\Документы\Денис\Перс%20данные\Политика%20обработки%20Пдн\Постановление(%20Пдн)\Приложение%205%20Политика%20информационной%20безопасности.doc) администрации, руководящие и нормативные документы ФСБ и ФСТЭК России.

1.4. Методическое руководство работой пользователя осуществляется администратором по безопасности средств защиты конфиденциальной информации.

## 2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите конфиденциально информации и распоряжений, регламентирующих порядок действий по защите конфиденциальной информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него Инструкцией пользователя автоматизированной системы.

2.3. Знать и соблюдать установленные требования по режиму обработки конфиденциальной информации, учету, хранению и пересылке носителей информации, обеспечению безопасности конфиденциальной информации, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях ограниченного доступа.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору.

2.8. Для получения консультаций по вопросам работы и настройке программных средств необходимо обращаться к Администратору по безопасности средств защиты конфиденциальной информации.

2.9. Пользователям запрещается:

Разглашать [конфиденциальную информацию](file:///D:\Документы\Денис\Перс%20данные\Политика%20обработки%20Пдн\Постановление(%20Пдн)\Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc) третьим лицам.

Копировать конфиденциальную информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты конфиденциальной информации.

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к конфиденциальной информации.

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты конфиденциальной информации.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения [внештатных и аварийных ситуаций](file:///D:\Документы\Денис\Перс%20данные\Политика%20обработки%20Пдн\Постановление(%20Пдн)\Приложение%2020%20Инструкция%20пользователя%20по%20обеспечению%20безопасности%20обработки%20персональных%20данных,%20при%20возникновении%20внештатных%20ситуаций.doc), с целью ликвидации их последствий, в рамках возложенных на него функций.

Приложение №6

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Руководство**

администратора по эксплуатации технических и программных средств защиты конфиденциальной информации в администрации муниципального образования Каировский сельсовет

Саракташского района Оренбургской области

## 1. Общие положения

1.1. Администратор в своей работе использует настоящее руководство, [Политику информационной безопасности](file:///G:\ТЗИ_дома\!!!_Чистовое%20на%20печать_!!!\Приложение%205%20Политика%20информационной%20безопасности.doc) администрации, руководящие и нормативные документы ФСБ ФСТЭК России.

1.2. Администратор отвечает за обеспечение устойчивой работоспособности технических и программных средств защиты конфиденциальной информации.

1.3. Методическое руководство работой Администратора осуществляется ответственным за обеспечение конфиденциальной информации.

## 2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите конфиденциальной информации и распоряжений, регламентирующих порядок действий по защите конфиденциальной информации.

2.2. Обеспечивать установку, настройку и своевременное обновление программных элементов защиты конфиденциальной информации:

программного обеспечения серверов (операционные системы);

программного обеспечения АРМ (прикладное и специальное ПО)

2.3. Обеспечивать работоспособность технических элементов защиты конфиденциальной информации.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках, возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов защиты конфиденциальной информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защите конфиденциальной информации, в пределах, возложенных на него функций.

2.8. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности конфиденциальной информации.

2.9. Информировать ответственного за обеспечение конфиденциальной информации о фактах нарушения установленного порядка эксплуатации технических и программных средств защиты конфиденциальной информации.

2.10. Требовать прекращения обработки конфиденциальной информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка эксплуатации технических и программных средств защиты.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности конфиденциальной информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки конфиденциальной информации, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.12. Присутствовать при выполнении технического обслуживания средств защиты конфиденциальной информации сторонними физическими людьми и организациями.

2.13. Принимать меры по реагированию, в случае возникновения [внештатных и аварийных ситуаций](file:///G:\ТЗИ_дома\!!!_Чистовое%20на%20печать_!!!\Приложение%2020%20Инструкция%20пользователя%20по%20обеспечению%20безопасности%20обработки%20персональных%20данных,%20при%20возникновении%20внештатных%20ситуаций.doc), с целью ликвидации их последствий.

2.14. Не допускать к работе на рабочих станциях и серверах посторонних лиц.

2.15. Участвовать в приемке для нужд новых программных средств.

2.16. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

2.17. При изменении конфигурации и состава средств защиты конфиденциальной информации вносить соответствующие изменения в паспорт АС, обрабатывающей конфиденциальную информацию.

Приложение №7

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Руководство**

пользователя по обеспечению безопасности информационной системы персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

## 1. Общие положения

1.1. Пользователь информационной системы персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник администрации Каировского сельсовета Саракташского района (далее – администрации), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4.Пользователь в своей работе руководствуется настоящей инструкцией, [Политикой информационной безопасности](../Политика%20обработки%20Пдн/Постановление(%20Пдн)/Приложение%205%20Политика%20информационной%20безопасности.doc) администрации, руководящими и нормативными документами ФСТЭК.

1.5. Методическое руководство работой пользователя осуществляется администратором ИСПДн.

## 2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него Инструкцией пользователя автоматизированной системы персональных данных (ПДн).

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

Разглашать [защищаемую информацию](../Политика%20обработки%20Пдн/Постановление(%20Пдн)/Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc) третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты информации.

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11.Принимать меры по реагированию, в случае возникновения [внештатных ситуаций и аварийных ситуаций](../Политика%20обработки%20Пдн/Постановление(%20Пдн)/Приложение%2020%20Инструкция%20пользователя%20по%20обеспечению%20безопасности%20обработки%20персональных%20данных,%20при%20возникновении%20внештатных%20ситуаций.doc), с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

## 3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других).

Передавать по Сети [защищаемую информацию](../Политика%20обработки%20Пдн/Постановление(%20Пдн)/Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc) без использования средств защиты каналов связи.

Запрещается скачивать из Сети программное обеспечение и другие файлы.

Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).

Запрещается нецелевое использование подключения к сети.

Приложение №8

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Руководство**

администратора по обеспечению безопасности информационной системы персональных данных в администрации Каировского сельсовета Саракташского района Оренбургской области

## 1. Общие положения

1.1.Администратор информационной системы персональных данных (ИСПДн) (далее – Администратор) назначается распоряжением главы Каировского сельсовета Саракташского района Оренбургской области.

1.2.Администратор в своей работе руководствуется настоящей инструкцией, [Политикой информационной безопасности](file:///D:\Документы\Денис\Перс%20данные\Политика%20обработки%20Пдн\Постановление(%20Пдн)\Приложение%205%20Политика%20информационной%20безопасности.doc) администрации, руководящими и нормативными документами ФСТЭК России.

1.3.Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.4.Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

## 2. Должностные обязанности

Администратор обязан:

2.1.Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2.Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);

аппаратных средств;

аппаратных и программных средств защиты.

2.3.Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4.Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5.Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6.В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7.Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

2.8.Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9.Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10.Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11.Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12.Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13.Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14.Принимать меры по реагированию, в случае возникновения [внештатных и аварийных ситуаций](file:///D:\Документы\Денис\Перс%20данные\Политика%20обработки%20Пдн\Постановление(%20Пдн)\Приложение%2020%20Инструкция%20пользователя%20по%20обеспечению%20безопасности%20обработки%20персональных%20данных,%20при%20возникновении%20внештатных%20ситуаций.doc), с целью ликвидации их последствий.

2.15.Не допускать к работе на рабочих станциях и серверах посторонних лиц.

2.16.Осуществлять контроль монтажа оборудования специалистами сторонних организаций.

2.17.Участвовать в приемке новых программных средств.

2.18. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

2.19.При изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС, обрабатывающей информацию ограниченного доступа.

Приложение №9

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

## Инструкция

по порядку учета и хранению съемных носителей конфиденциальной информации и персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района

Оренбургской области

## 1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом №149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и устанавливает порядок использования носителей информации, предоставляемых в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – администрации) для использования в информационных системах.

1.2. Действие настоящей Инструкции распространяется на всех сотрудников администрации.

## 2. Основные термины, сокращения и определения

**1. Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения, и оборудования вычислительной техники.

**2. АРМ** – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

**3. ИБ** – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

**4. ИС** – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

**5. Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.

**6. Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

**7. ПК** – персональный компьютер.

**ПО** – программное обеспечение вычислительной техники.

**8. ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

**9. ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

**10. Пользователь** – работник администрации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

## 3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС администрации понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью администрации и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным в администрации носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители конфиденциальной информации предоставляются сотрудникам администрации по инициативе Руководителей структурных подразделений в случаях:

* необходимости выполнения вновь принятым работником своих должностных обязанностей;
* возникновения у сотрудника органа местного самоуправления производственной необходимости.

**4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации**

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в администрации подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляет администратор. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.3.1. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению № 1 к настоящей Инструкции.

4.4. При использовании сотрудниками носителей конфиденциальной информации (персональных данных) необходимо:

- соблюдать требования настоящей Инструкции;

- использовать носители информации исключительно для выполнения своих служебных обязанностей;

- ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции;

- бережно относится к носителям конфиденциальной информации (персональных данных);

- обеспечивать физическую безопасность носителей конфиденциальной информации (персональных данных) всеми разумными способами;

- извещать администраторов ИС о фактах утраты (кражи) носителей конфиденциальной информации (персональных данных).

4.5. При использовании носителей конфиденциальной информации (персональных данных) запрещено:

- использовать носители конфиденциальной информации (персональных данных) в личных целях;

- передавать носители конфиденциальной информации (персональных данных) другим лицам (за исключением администраторов ИС);

- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

4.6. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником администрации между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.

4.7. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.8. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.9. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.10. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

4.11. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме.

4.12. В случае увольнения или перевода работника в другую организацию, предоставленные носители конфиденциальной информации изымаются.

## 5. Ответственность

Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами органа исполнительной власти.

Приложение

к Инструкции по порядку учета и хранению съемных носителей конфиденциальной информации и персональных данных в администрации Каировского сельсовета Саракташского района Оренбургской области

Журнал

учета электронных носителей персональных данных

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Начат: | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г. |
| Окончен: | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г. |
| На \_\_\_\_ листах | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Регистрационный (учетный) номер носителя | Вид носителя | Тип носителя и его емкость | Дата поступления |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения | Дата и номер акта об уничтожении | Примечание |
| 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |

Приложение №10

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

## Инструкция

пользователя автоматизированной системы в администрации муниципального образования Каировский сельсовет

Саракташского района Оренбургской области

Каждый сотрудник, участвующий в рамках своих должностных обязанностей в процессах обработки конфиденциальных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы (АС), несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах АС;

- хранить в тайне свой пароль (пароли). В соответствии с установленной периодичностью менять свой пароль (пароли);

- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить администратора АС в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках средств вычислительной техники (СВТ) или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к данным, защищаемым СВТ;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на компьютеры технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку конфиденциальных данных в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и бумажные документы, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства АС так, чтобы с них существовала возможность визуального считывания информации.

Приложение №11

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

## Инструкция

администратора автоматизированной системы по безопасности конфиденциальной информации в администрации муниципального образования Каировский сельсовет Саракташского района

Оренбургской области

1. Администратор автоматизированной системы (АС) обязан:

- знать состав основных и вспомогательных технических систем, и средств (далее - ОТСС и ВТСС) установленных и смонтированных в АС, перечень используемого программного обеспечения (далее - ПО) в АС;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в АС СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей АС в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в АС;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- контролировать своевременное (не реже чем один раз в год) проведение смены паролей для доступа пользователей к компьютерам и ресурсам АС;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в АС;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в АС;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в АС;

- периодически тестировать функции средств защиты информации (СЗИ) от несанкционированного доступа (НСД), особенно при изменении программной среды и полномочий исполнителей;

- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств АС;

- контролировать соответствие документально утвержденного состава аппаратной и программной части АС реальным конфигурациям АС, вести учет изменений аппаратно-программной конфигурации;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АС и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

- вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ, выполнения профилактических работ, установки и модификации аппаратных и программных средств СВТ;

- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать главе муниципального образования о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

- вести документацию на АС в соответствии с требованиями нормативных документов.

2. Администратор АС имеет право:

- требовать от сотрудников - пользователей АС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в АС;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов АС;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

Приложение №12

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

Инструкция

о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

**1. Общие положения**

1.1. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и систем защиты информации определяет действия, связанные с функционированием информационных систем персональных данных (далее – ИСПДн) администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящей инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения ИСПДн (далее – Инструкции) является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации, определение мер защиты от потери информации, определение действий восстановления в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

1.4. Ответственными сотрудниками за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначаются:

- сотрудники, обрабатывающие персональные данные;

- руководители структурных подразделений, в которых производится обработка персональных данных;

- сотрудники ответственные за защиту персональных данных при обработке в ИСПДн.

**2. Порядок реагирования на инцидент**

2.1. В настоящей Инструкции под инцидентом понимается любое происшествие, связанное со сбоем в функционировании элементов ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;

- в результате преднамеренных действий пользователей и третьих лиц;

- в результате нарушения правил эксплуатации технических и программных средств ИСПДн;

- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с непосредственным руководителем. По необходимости, иерархия согласования может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

**3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов**

3.1. Техническими мерами для обеспечения непрерывной работы и восстановления являются программные, аппаратные и технические средства и системы, используемые для предотвращения потери информации, такие как:

- системы жизнеобеспечения ИСПДн;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

3.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы резервного питания.

3.3. Все помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн: ПЭВМ, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания.

3.5. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.6. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердых носителях (жесткий магнитный диск, лазерный диск, Flash-накопитель).

3.7. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже 1 раза в неделю;

- для технологической информации – не реже 1 раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты) каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.8. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Приложение №13

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Перечень**

сведений конфиденциального характера, подлежащих защите в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

**1. Общие положения**

1.1. Настоящий Перечень разработан на основании и в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации ",[Указом Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера"](http://docs.cntd.ru/document/9039120).

1.2. Настоящий Перечень предназначен для государственных служащих - работников структурных подразделений администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – администрации), выполнение должностных обязанностей которых связано с использованием сведений конфиденциального характера.

1.3. Перечень может пересматриваться по мере необходимости, уточняться и дополняться установленным порядком.

**2. Сведения конфиденциального характера**

В настоящем перечне предусматриваются категории сведений, представляющих конфиденциальную информацию, персональные данные, разглашение которых может нанести материальный, моральный или иной ущерб интересам субъекта данных сведений либо администрации в целом. К таким сведениям относятся:

1) сведения в области информатизации и защиты информации:

- сведения об особенностях используемых технологий и специфике их применения;

- сведения о порядке и состоянии организации охраны, системе сигнализации, шифрах, паролях;

- сведения об информационной системе и применяемых способах информационной защиты;

- сведения о программном обеспечении, принципах построения, структуре и составе оборудования информационной системы;

- принципы организации электронного и бумажного документооборота;

- методы и способы защиты конфиденциальной информации от утечки, утери или искажения;

- система организации и разграничения доступа в автоматизированной системе, идентификаторы и пароли, используемые сотрудниками для доступа к информации;

2) Военно-мобилизационные вопросы, вопросы ГО:

- сведения по вопросам мобилизационной подготовки, не раскрывающие обобщенные данные в целом по организации;

- сведения по наличию запасов мобилизационного резерва в отдельных организациях, не раскрывающие обобщенные данные в целом по организации;

- сведения по испытанию защитных или специальных сооружений ГО на соответствие санитарно-гигиеническим и санитарно-техническим нормам;

- сведения по учету и бронированию военнообязанных по отдельным организациям, в которых работает военнообязанных менее 300 человек;

- аналитические справки, письма, телеграммы и другие материалы по учету и бронированию военнообязанных;

- материалы переписки по воинским частям в части их дислокации, штатной численности, укомплектованности;

3) Персональные данные:

- сведения о фактах, событиях и обстоятельствах частной жизни сотрудников администрации, позволяющие идентифицировать их личность (персональные данные);

- сведения, содержащиеся в книгах записей актов гражданского состояния или в метрических книгах о рождении, заключении брака, расторжении брака, смерти, усыновлении, установлении отцовства, перемене фамилии, имени, отчества;

- списки со сведениями на детей (от 0 до 18 лет), оставшихся без попечения родителей и подлежащих устройству в семью (передачу под опеку, на усыновление, удочерение) с указанием индивидуальных внешних данных и психологических характеристик детей, медицинских сведений, данных о месте и времени рождения, родителях, обстоятельствах лишения родительских прав

- другая документированная информация, содержащая сведения о фактах, событиях и обстоятельствах частной жизни граждан, позволяющая идентифицировать их личность, за исключением сведений, подлежащих распространению в средствах массовой информации в соответствии с законодательством;

4) Финансово-экономические сведения:

- сведения о бухгалтерском учете (за исключением годового баланса);

- сведения о финансовых операциях;

- сведения о величине доходов и расходов, о состоянии дебиторской и кредиторской задолженностях (за исключением годового баланса);

- сведения, содержащиеся в финансово - договорных схемах администрации;

- порядок начисления и сроки выплат по заработной плате, а также факты и размеры задолженностей по заработной плате;

5) Прочие сведения:

- размещение, размеры, характеристики, условия эксплуатации зданий и помещений;

- уровень и объем транспортно-технического обеспечения;

- материалы внутренних и внешних ревизий;

- сведения о предметах и целях совещаний;

- входящая и исходящая корреспонденция (в том числе в электронном виде), за исключением официально публикуемых материалов;

- планы помещений и порядок доступа в них;

- порядок и места хранения архивных документов;

- система и способы обеспечения общей безопасности объектов и администрации в целом;

- штатное расписание администрации или муниципальных образований;

- полный список телефонов, включая домашние, сотрудников организации с указанием их занимаемой должности;

- информация по гражданским, административным делам;

- другие служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

Приложение №14

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

Правила

рассмотрения запросов субъектов персональных данных или их представителей в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее - администрации) разработаны в соответствии с Федеральным [законом](consultantplus://offline/ref=48940DEAD8B81658F0918E909625E89CA4C483957E49183E1A806E41F7X316B) от 27 июля 2006 года № 152-ФЗ "О персональных данных", [постановлением](consultantplus://offline/ref=48940DEAD8B81658F0918E909625E89CA4C78396774E183E1A806E41F7X316B) Правительства Российской Федерации от 21 марта 2012 года № 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», определяют сроки и последовательность действий, порядок взаимодействия между структурными подразделениями и должностными лицами администрации запросов субъектов персональных данных или их представителей.

2. В настоящих Правилах используются основные понятия, установленные Федеральный законом от 27 июля 2006 года № 152- ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

3. Субъектами персональных данных в администрации являются работники администрации, лица, претендующие на замещение вакантных должностей муниципальной службы в администрации и (или) состоящие в кадровом резерве администрации, лица, ранее состоявшие на муниципальной службе в администрации, личные дела которых не переданы на хранение в муниципальный архив.

4. Представитель субъекта персональных данных - лицо, действующее от имени субъекта персональных данных в силу полномочия, основанного на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления.

5. Субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона № 152-ФЗ;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ и другими нормативными правовыми актами.

6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

7. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.Основанием для предоставления сведений, предусмотренных пунктом 5 настоящих Правил, является обращение субъекта персональных данных или его представителя в администрацию лично либо получение администрацией запроса субъекта персональных данных или его представителя через организации федеральной почтовой связи. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

2) сведения о дате выдачи указанного документа и выдавшем его органе;

3) сведения, подтверждающие участие субъекта персональных данных в отношениях с администрацией (реквизиты акта о назначении на должность либо увольнении с должности, решения конкурсной комиссии о зачислении в кадровый резерв и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных администрацией;

4) подпись субъекта персональных данных или его представителя.

10. В день поступления запроса субъекта персональных данных или его представителя указанный запрос регистрируется и после проставления соответствующей визы руководителя администрации передается запрос в отдел кадров администрации для исполнения.

11.Отдел кадров администрации обеспечивает рассмотрение запроса, сообщение субъекту персональных данных или его представителю информации о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, подготовку необходимой информации, а также предоставление возможности ознакомления субъекта персональных данных или его представителя с этой информацией в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

12. Информация должна быть предоставлена субъекту персональных данных или его представителю в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

13. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных, субъекту персональных данных или его представителю при получении запроса субъекта персональных данных или его представителя отдел кадров обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение [пункта 6](consultantplus://offline/ref=D4EDBE38979E53341484D492EA043CBF337EDA01DFC33C05FA58A98BE01D8789E272DE5B1C28A149D17222K0qEC) настоящих правил, [части 8 статьи 14](consultantplus://offline/ref=D4EDBE38979E53341484CA9FFC6866B333748309D1C63556A007F2D6B7148DDEA53D87195825A34AKDq4C) Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

14. В случае если информация, указанная в пункте 5 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения информации, указанной в пункте 5 настоящих Правил, и ознакомления с ней, не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

15. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения информации, указанной в пункте 5 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного выше, в случае, если такая информация и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду с информацией, указанной ранее, должен содержать обоснование направления повторного запроса.

16. В случае отказа субъекту персональных данных или его представителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным [пунктами](consultantplus://offline/ref=D4EDBE38979E53341484D492EA043CBF337EDA01DFC33C05FA58A98BE01D8789E272DE5B1C28A149D17223K0qDC) 14, 15 настоящих правил, администрация дает мотивированный ответ, в котором указывает основания для отказа.

17. Администрация предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

18. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, администрация вносит в них необходимые изменения.

19. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, администрация уничтожает такие персональные данные, при этом уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

20. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных администрация обязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

Приложение №15

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

Правила

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее - администрации) разработаны в соответствии с Федеральным законом от 27 июля 2006 года   
№ 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 года № 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», иными нормативными правовыми актами (далее – Правила), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных субъекта персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации.

2. В настоящих Правилах используются основные понятия и термины, установленные Федеральным [законом](consultantplus://offline/ref=0AB76CC07DAC348E0003252618D478DE49A653541FBD36359D7D8DD6BE6332H) от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон № 152-ФЗ).

3. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации осуществляется путем проведения плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

4. Плановые проверки проводятся на основании утвержденного распоряжением администрации ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных в администрации требованиям к защите персональных данных, установленных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами (далее – План).

В [Плане](consultantplus://offline/ref=9978311543A9ED2F68D3B77D673B2F65E22FFC4C756945E12B7BD5A2A91F2D30DB7968DEC137286685C944zCu6C) по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

5. Основанием для проведения внеплановой проверки является поступившее письменное обращение (жалоба) субъекта персональных данных или его представителя о нарушении правил обработки персональных данных.

Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления обращения (жалобы).

6. Проверки проводятся постоянно действующей комиссией по контролю за обработкой персональных данных, образованной распоряжением от 15.07.2021г № 76-р “О создании и организации работы комиссии по уничтожению документов, содержащих персональные данные”. В проведении проверки не может участвовать муниципальный служащий, прямо или косвенно заинтересованный в ее результатах.

7. В ходе проведения Проверки комиссией полностью, объективно и всесторонне изучаются следующие вопросы:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных субъекта персональных данных при их обработке, необходимых для выполнения требований по защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных субъекта персональных данных;

2) порядок и условия применения средств защиты информации;

3) состояние учета машинных носителей персональных данных субъекта персональных данных;

4) соблюдение правил доступа к персональным данным субъекта персональных данных;

5) наличие (отсутствие) фактов несанкционированного доступа к персональным данным субъекта персональных данных и принятие необходимых мер;

6) мероприятия по восстановлению персональных данных субъекта персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7) осуществление мероприятий по обеспечению целостности персональных данных субъекта персональных данных.

8. Комиссия имеет право:

1) запрашивать у должностных лиц информацию, необходимую для реализации полномочий;

2) требовать от должностных лиц, замещение должностей которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным субъектов персональных данных, уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных субъекта персональных данных;

3) принимать меры по приостановлению или прекращению обработки персональных данных субъекта персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

4) вносить руководителю предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных субъекта персональных данных при их обработке;

5) вносить руководителю предложения о привлечении лиц, виновных в нарушении требований Федерального закона № 152-ФЗ и принятых в соответствии с ним нормативных правовых актов, к ответственности, предусмотренной законодательством Российской Федерации.

9. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

10. Срок проведения проверки устанавливается распоряжением администрации и не превышает месяц со дня принятия решения о ее проведении.

11. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, комиссия подготавливает письменное заключение.

12. По существу поставленных в обращении (жалобе) вопросов комиссия в течение пяти рабочих дней со дня окончания проверки дает письменный ответ заявителю.

Приложение №16

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

Правила

работы с обезличенными персональными данными в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области

Настоящие Правила работы с обезличенными персональными данными в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее - Правила) разработаны в соответствии Федеральным [законом](consultantplus://offline/ref=65A6843494D0961C3B09DA3486E02484E0535D69961D9AFBC33667FF94gDq0C) от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее - Федеральный закон № 152-ФЗ), [постановлением](consultantplus://offline/ref=65A6843494D0961C3B09DA3486E02484E0505D6A9F1A9AFBC33667FF94gDq0C) Правительства Российской Федерации от 21 марта 2012 года № 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" и определяют порядок работы с обезличенными персональными данными в администрации.

2. В соответствии с Федеральным [законом](consultantplus://offline/ref=65A6843494D0961C3B09DA3486E02484E0535D69961D9AFBC33667FF94gDq0C) № 152-ФЗ:

-персональные данные - 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;

-обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Обезличивание персональных данных в администрации проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных.

4. Способами обезличивания персональных данных при условии их дальнейшей обработки являются:

- уменьшение перечня обрабатываемых сведений;

- замена части сведений идентификаторами;

- обобщение - понижение точности некоторых сведений;

- понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

- деление сведений на части и обработка в разных информационных системах;

- другие способы.

5. Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

7. Обезличенные персональные данные обрабатываются с использованием и без использования средств автоматизации.

8. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями (если они используются);

- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем.

9. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;

- правил доступа к ним и в помещения, где они хранятся.

Приложение №17

к постановлению

администрации

Каировского сельсовета

от 14.02.2023 №11-п

**Положение**

**об обработке персональных данных сотрудников**

**1. Общие положения**

1.1. Положение определяет порядок обработки в администрации муниципального образования Каировский сельсовет Саракташского района Оренбургской области (далее – администрация) персональных данных сотрудников (далее - сотрудники).

1.2. Под персональными данными сотрудника понимается информация, необходимая администрации в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

1.3. Под обработкой персональных данных понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработка персональных данных сотрудников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Совокупность персональных данных сотрудника, позволяющая идентифицировать его личность, относится к конфиденциальной информации, за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей с персональными данными осуществляется в соответствии с действующими в администрации документами.

1.4. Администрация является оператором персональных данных лиц, указанных в пункте 1.1. настоящего Положения. На основании договора администрация может поручить обработку персональных данных третьим лицам. Существенным условием договора об оказании услуг по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности персональных данных и безопасности персональных данных при их обработке.

1.5. Объем и содержание обрабатываемых персональных данных регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», другими федеральными законами.

1.6. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, администрация вправе получать и обрабатывать данные о частной жизни сотрудника только с его согласия.

Администрации не имеет права получать и обрабатывать персональные данные сотрудника об их членстве в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

**2. Порядок обработки персональных данных сотрудников**

2.1. Администрация все персональные данные сотрудников получает у них самих. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие на их получение. Администрация сообщает сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных, последствиях отказа сотрудника дать письменное согласие на их получение.

2.2. Персональные данные сотрудников администрации обрабатываются:

**-** отделом кадров;

- бухгалтерией;

- самим сотрудником, носителем данных.

Перечень должностей сотрудников, допущенных к персональным данным, и объём персональных данных, к которым они допускаются, утверждается распоряжением главы муниципального образования.

2.3. Указанные в 2.2 настоящего Положения лица осуществляют обработку, включая сбор, накопление, систематизацию, уточнение, передачу персональных данных сотрудников в объёмах и целях, предусмотренных законодательством Российской Федерации и локальными нормативными актами администрации муниципального образования, а также обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

2.4. Персональные данные хранятся:

- в электронном виде (на серверах, персональных компьютерах, а также на сменных магнитных, оптических и других цифровых носителях);

- на бумажных носителях, в том числе в личных делах сотрудников, специально оборудованных шкафах и сейфах.

2.5. При принятии решений, затрагивающих интересы сотрудника, администрация не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения, в том числе на цифровых носителях.

2.6. Защита персональных данных сотрудников от неправомерного их использования или утраты обеспечивается администрацией за счёт собственных средств в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности, целостности и доступности.

2.7. Сотрудники и их представители должны быть ознакомлены под роспись с настоящим Положением и другими документами администрации, устанавливающими порядок обработки персональных данных сотрудников, а также об их правах и обязанностях в этой области.

**3. Ведение личных дел**

3.1. Персональные данные и иные сведения, связанные с приёмом на работу, трудовой деятельностью и увольнением, вносятся в личное дело сотрудника администрации в связи с трудовыми отношениями. Личные дела сотрудников ведутся специалистом по кадрам.

3.2. Совокупность персональных данных, внесенных в личные дела сотрудников, и иные сведения, содержащиеся в личных делах сотрудников, относятся к сведениям конфиденциального характера. На личное дело сотрудника ставится гриф «Конфиденциально», на документы, хранящиеся в личном деле, гриф не проставляется.

3.3. К личному делу сотрудников приобщаются:

а) письменное заявление о приеме на работу;

б) собственноручно заполненная и подписанная сотрудником анкета, установленной формы с приложением фотографии;

в) копия паспорта;

г) копия трудовой книжки;

д) копия свидетельства о государственной регистрации актов гражданского состояния;

е) копия документов о профессиональном образовании, персональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

ж) копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);

з) копия распоряжения о приеме на работу;

и) экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;

к) копии распоряжений о переводе сотрудников на другую постоянную работу, о переводе на другую работу временно;

л) копии распоряжений о расторжении трудового договора;

м) аттестационный лист сотрудника, прошедшего аттестацию;

н) копии документов о присвоении сотруднику квалификационного разряда;

о) копии распоряжений о поощрении сотрудника, а также о применении к нему дисциплинарного взыскания до его снятия или отмены;

п) документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений;

р) копия страхового свидетельства обязательного пенсионного страхования;

с) копия военного билета.

3.4. В личное дело сотрудника вносятся также письменные объяснения сотрудника, если такие объяснения даны им после ознакомления с документами своего личного дела.

3.5. Документы, приобщенные к личному делу сотрудника, брошюруются, страницы нумеруются, к личному делу прилагается опись.

3.6. В обязанности специалиста по кадрам, осуществляющего ведение личных дел сотрудников, входит:

а) формирование и обеспечение сохранности личных дел сотрудников;

б) обеспечение конфиденциальности сведений, содержащихся в личных делах сотрудников, в соответствии с законодательством Российской Федерации и внутренними документами администрации.

в) ознакомление сотрудника с документами своего личного дела во всех случаях, предусмотренных законодательством Российской Федерации.

3.7. Специалист по кадрам, уполномоченный на ведение и хранение личных дел сотрудников администрации, привлекаются в соответствии с законодательством Российской Федерации к дисциплинарной и иной ответственности за разглашение конфиденциальных сведений, содержащихся в указанных личных делах.

3.8. Личные дела уволенных сотрудников хранятся специалистом по кадрам в течение двух лет со дня увольнения, после чего передаются в архив.

**4. Передача персональных данных третьим лицам.**

**Обработка персональных данных лиц, не состоящих с администрацией в трудовых отношениях**

4.1. При обработке персональных данных администрация обязана соблюдать следующие требования:

4.1.1. Не сообщать персональные данные сотрудника третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных Трудовым кодексом Российской Федерации и иными федеральными законами.

4.1.2. Не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия.

4.1.3. Не запрашивать информацию о состоянии здоровья сотрудника, за исключением сведений, необходимых для установления возможности выполнения сотрудником трудовых функций.

4.1.4. Предупреждать лиц, получающих персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные сотрудника, обязаны соблюдать режим конфиденциальности в отношении этих данных.

4.2 Передача персональных данных сотрудников негосударственному пенсионному фонду и страховой компании в целях выполнения в отношении сотрудников условий Положения о социальном обеспечении сотрудников администрации осуществляется в соответствии с заключенными с этими организациями договорами и соглашениями о конфиденциальности при наличии письменного согласия сотрудников.

4.3 Администрация может получать и обрабатывать с соблюдением требований законодательства Российской Федерации и настоящего положения персональные данные следующих категорий лиц:

- кандидатов для приема на работу в администрацию при наличии их письменного согласия.

Права указанных лиц в отношении обработки их персональных данных, хранящихся в Учреждении, определяются законодательством Российской Федерации и разделом 7 настоящего Положения.

**5. Организация доступа к персональным данным**

5.1 Защита персональных данных в администрации предусматривает ограничение к ним доступа.

5.2 Доступ к персональным данным разрешается только лицам, определенным в порядке, установленным пунктом 2.2 настоящего Положения. При этом указанные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций, и в целях, для которых они сообщены.

5.3 Руководитель администрации, осуществляющий обработку персональных данных:

- несет ответственность за организацию защиты персональных данных;

- закрепляет за сотрудниками, допущенными к обработке персональных данных, конкретные массивы носителей с персональными данными, которые необходимы для выполнения возложенных на них функций;

- организует изучение уполномоченными сотрудниками нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

- обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном отделении;

- организует контроль доступа к персональным данным в соответствии с функциональными обязанностями того или иного сотрудника отделения.

5.4. С сотрудником, допущенным к персональным данным, заключается соглашение о допуске к конфиденциальной информации в установленном порядке. Существенным условием соглашения является обязательство сотрудника перед администрацией о нераспространении доверенных ему персональных данных. Соглашение от имени администрации подписывается главой муниципального образования.

5.5. К числу массовых потребителей персональных данных вне Учреждения относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;

- правоохранительные органы;

- органы статистики;

- страховые агентства;

- военные комиссариаты;

- органы социального страхования;

- пенсионные фонды;

- подразделения муниципальных органов управления.

Доступ представителей государственных органов к персональным данным регламентируется законодательством Российской Федерации.

5.6. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления сотрудника.

5.7. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

**6.** **Обязанности лиц, допущенных к обработке персональных данных сотрудника**

6.1. Лица, допущенные к работе с персональными данными обязаны:

- знать законодательство Российской Федерации и нормативные документы администрации;

- обеспечивать сохранность закрепленного массива носителей с персональными данными, исключать возможность ознакомления с ними других лиц;

- докладывать своему непосредственному руководителю обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

**7. Права сотрудников при обработке персональных данных, хранящихся в администрации**

7.1. Сотрудники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса Российской Федерации или иного федерального закона;

- дополнение своих персональных данных оценочного характера заявлением, выражающим собственную точку зрения сотрудника;

- требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведённых в них исключениях, исправлениях или дополнениях;

- участие в разработке мер защиты персональных данных;

- обжалование в суд любых неправомерных действий или бездействия при обработке и защите его персональных данных.

**8. Защита персональных данных сотрудников**

8.1. В целях обеспечения сохранности и конфиденциальности персональных данных сотрудников администрации все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками отдела по работе с персоналом, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

8.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке администрации муниципального образования и в том объёме, который позволяет не разглашать излишний объём персональных сведений о сотрудниках Учреждения.

8.3. Передача информации, содержащей сведения о персональных данных сотрудников Учреждения по телефону, факсу, электронной почте без письменного согласия сотрудника запрещается.

8.4. Личные дела и документы, содержащие персональные данные сотрудников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

8.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

**9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных сотрудника**

9.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.