**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ**

**ХУТОРСКОЙ СЕЛЬСОВЕТ**

**НОВОСЕРГИЕВСКОГО РАЙОНА**

**ОРЕНБУРГСКОЙ ОБЛАСТИ**

**ПОСТАНОВЛЕНИЕ**

**23 июня 2017 год № 32-п.**

**с. Хуторка**

«Об утверждении Политики информационной безопасности

в отношении обработки персональных данных администрации МО

«Хуторской сельсовет» Новосергиевского района Оренбургской области»

В целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления 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 и муниципальными органами». В соответствии с Постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51 «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»:

1.Утвердить Политику информационной безопасности в отношении обработки персональных данных в администрации Хуторского сельсовета Новосергиевского района Оренбургской области согласно приложению.

2. Контроль за исполнением настоящего постановления оставляю за собой.

3. Постановление вступает в силу со дня его подписания и подлежит размещению на официальном сайте администрации муниципального образования «Хуторской сельсовет» Новосергиевского района Оренбургской области.

Глава администрации Хуторского сельсовета А.Ф. Михайлов

Разослано: в дело, отделу кадров, прокурору.

Приложение

к постановлению администрации

муниципального образования Хуторской сельсовет Новосергиевского района

Оренбургской области

от 23.06.2017 г. № 32-п.

Политика

информационной безопасности в отношении обработки персональных данных в администрации муниципального образования

«Хуторской сельсовет» Новосергиевского района Оренбургской области

1. Общие положения

Политика информационной безопасности (далее – Политика) администрации муниципального образования «Хуторской сельсовет» Новосергиевского 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 15.02.08 г.
8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15.02.08 г.
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 администрации.

**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. Список соответствия функций подсистем СЗПДн уровню защищенности представлен в Приложении.

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 передачи 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, непосредственный начальник соответствующего подразделения 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.

Сотрудник, вновь поступивший на должность, обязан пройти инструктаж по безопасности персональных данных и защите конфиденциальной информации, со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн в отделе по координации административной реформы и информационным технологиям.

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, руководству подразделения и лицу, отвечающему за обеспечение безопасности ПДн.

**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 РФ 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.