АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГУСЬ-ХРУСТАЛЬНЫЙ РАЙОН
(МУНИЦИПАЛЬНЫЙ РАЙОН) ВЛАДИМИРСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

22.06.2012 № 939

в редакции

28.02.2023 № 241

О политике администрации муниципального образования Гусь-Хрустальный район (муниципальный район) Владимирской области в отношении обработки персональных данных

В целях обеспечения защиты персональных данных граждан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и на основании Устава Гусь-Хрустального района

П О С Т А Н О В Л Я Ю :

1. Утвердить Политику администрации муниципального образования Гусь-Хрустальный район (муниципальный район) Владимирской области в отношении обработки персональных данных (приложение).

2. Контроль за исполнением настоящего постановления оставляю за собой.

3. Настоящее постановление вступает в силу со дня его официального опубликования и подлежит размещению на официальном сайте администрации района.

4. Опубликовать настоящее постановление в газете «Гусевские вести».

Глава района А.В. Кабенкин

Приложение
к постановлению администрации района
от 22.06.2012 № 939
(ред. от 28.02.2023 № 241)

ПОЛИТИКА
администрации муниципального образования Гусь-Хрустальный район (муниципальный район) Владимирской области в отношении обработки персональных данных

1. Термины и определения

Персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

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

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Информационная система персональных данных (далее - ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Общие положения

2.1. Настоящая Политика в отношении обработки персональных данных в администрации муниципального образования Гусь-Хрустальный район (муниципальный район) Владимирской области (далее – администрация района) составлена в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением 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».

2.2. Администрация района является оператором ПДн и внесена в реестр операторов, осуществляющих обработку ПДн.

2.3. Целью Политики в отношении обработки ПДн в администрации района (далее - Политика) является обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн Администрацией района.

2.4. Политика подлежит пересмотру в ходе периодического анализа со стороны Администрации района, а также в случаях изменения законодательства Российской Федерации в области персональных данных.

2.5. Политика подлежит опубликованию на официальном сайте Администрации района.

3. Область действия

3.1. Положения настоящей Политики распространяются на отношения, связанные с обработкой ПДн, осуществляемой Администрацией района:

– с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск ПДн, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях ПДн, и (или) доступ к таким ПДн;

– без использования средств автоматизации.

4. Цели обработки персональных данных

4.1. Обработка персональных данных осуществляется администрацией района в следующих целях:

– выполнение требований трудового законодательства Российской Федерации и законодательства о муниципальной службе в Российской Федерации в части ведения бухгалтерского учета, выполнение требований договора гражданско-правового характера, осуществление расчета заработной платы и иных выплат и удержаний, осуществления платежей и переводов в интересах субъекта ПДн; выполнения требований трудового законодательства Российской Федерации и законодательства о муниципальной службе в Российской Федерации в части ведения

кадрового учета, содействия в трудоустройстве, получении образования и продвижения по службе; ведение воинского учета;

– осуществление и выполнение возложенных законодательством Российской Федерации на Администрацию района функций, полномочий и обязанностей по предоставлению муниципальных услуг;

– рассмотрение обращений граждан;

– ведение дел об административных правонарушениях комиссией по делам несовершеннолетних и административной комиссией администрации района.

5. Правовые обоснования обработки персональных данных

5.1. Основанием обработки ПДн в администрации района являются следующие нормативные акты и документы:

– Конституция Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Кодекс Российской Федерации об административных правонарушениях;

– Уголовно-исполнительный кодекс Российской Федерации;

– Бюджетный кодекс Российской Федерации;

– Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

– Закон Владимирской области от 30.05.2007 № 58ОЗ «О муниципальной службе во Владимирской области»;

– Федеральный закон от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»;

– Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

– Федеральный закон от 15.12.2001 № 166-ФЗ «О государственном пенсионном обеспечении в Российской Федерации»;

– Федеральный закон от 28.12.2013 № 400-ФЗ «О страховых пенсиях»;

– Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве»;

– Федеральный закон от 21.07.1997 № 118-ФЗ «Об органах принудительного исполнения Российской Федерации»;

– Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

– Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

– Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

– Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

– Федеральный закон от 24.06.1999 № 120-ФЗ «Об основах системы профи-

лактики безнадзорности и правонарушений несовершеннолетних»;

– Федеральный закон от 21.12.1996 № 159-ФЗ «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей»;

– Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;

– Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;

– 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»;

– Постановление Правительства Российской Федерации от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;

– Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;

– Закон Владимирской области от 14.02.2003 № 11-ОЗ «Об административных правонарушениях во Владимирской области»;

– Закон Владимирской области от 10.10.2005 № 145-ОЗ «О наделении органов местного самоуправления отдельными государственными полномочиями Владимирской области по образованию и организации деятельности комиссий о делам несовершеннолетних и защите их прав»;

– Постановление администрации Владимирской области от 13.02.2020 № 70 «О мерах по реализации Закона Владимирской области от 10.10.2005 № 145-ОЗ «О наделении органов местного самоуправления отдельными государственными полномочиями Владимирской области по образованию и организации деятельности комиссий о делам несовершеннолетних и защите их прав»»;

– Закон Владимирской области от 02.10.2017 № 80-ОЗ «О комиссиях по делам несовершеннолетних и защите их прав во Владимирской области»;

– Закон Владимирской области от 30.12.2002 № 141- ОЗ «Об административных комиссиях»;

– Закон Владимирской области от 12.06.2006 № 96-ОЗ «О наделении органов местного самоуправления Владимирской области отдельными государственными полномочиями по вопросам административного законодательства»;

– Постановление Губернатора Владимирской области от 27.01.2006 № 51 «Об утверждении Положения о едином банке данных о несовершеннолетних, находящихся в социально опасном положении, и их семьях»;

– Постановление администрации Владимирской области от 17.06.2020 № 379 «Об утверждении Порядка рассмотрения муниципальными комиссиями по делам несовершеннолетних и защите их прав материалов (дел), не связанных с делами об административных правонарушениях»;

– Постановление администрации района от 06.10.2008 № 1380 «Об утвер-

ждении Положения о порядке формирования резерва кадров на замещение вакантных должностей муниципальной службы администрации муниципального образования Гусь-Хрустальный район»;

– Инструкция по работе с документами в администрации муниципального образования Гусь-Хрустальный район (муниципальный район);

– Постановление администрации района от 12.03.2012 № 328 «Об утверждении административного регламента предоставления муниципальной услуги «Предоставление мер социальной поддержки гражданам, пострадавшим от пожара или стихийных бедствий»»;

– Постановление администрации района от 21.05.2013 № 853 «Об утверждении административного регламента предоставления муниципальной услуги по выдаче заверенных копий документов, подлинники которых находятся в распоряжении администрации муниципального образования Гусь-Хрустальный район»;

– Постановление администрации района от 13.03.2009 № 264 «Об утверждении Административного регламента предоставления государственной услуги по обеспечению жильем отдельных категорий граждан, предусмотренных федеральными законами «О ветеранах», «О социальной защите инвалидов в Российской Федерации»»;

– Постановление администрации района от 29.12.2012 № 2051 «Об утверждении административного регламента предоставления администрацией муниципального образования Гусь-Хрустальный район (муниципальный район) муниципальной услуги по назначению муниципальной пенсии за выслугу лет лицам, замещавшим муниципальные должности на постоянной основе, и лицам, замещавшим должности муниципальной службы в муниципальном образовании Гусь-Хрустальный район»;

– Постановление администрации района от 17.12.2019 № 1470 «Об утверждении административного регламента предоставления муниципальной услуги по назначению ежемесячной денежной выплаты гражданам, удостоенным звания «Почётный гражданин Гусь-Хрустального района»»;

– Постановление администрации района от 22.01.2020 № 63 «Об утверждении Административного регламента предоставления государственной услуги «Предоставление государственных жилищных сертификатов на приобретение жилых помещений»»;

– Постановление администрации района от 13.01.2020 № 23 «Об утверждении Административного регламента предоставления муниципальной услуги «Предоставление отдельным категориям граждан социальных выплат на приобретение (строительство) жилья»»;

– Постановление администрации района от 13.01.2020 № 22 «Об утверждении Административного регламента предоставления муниципальной услуги «Предоставление жилых помещений специализированного жилищного фонда детям-сиротам и детям, оставшимся без попечения родителей, лицам из числа детей-сирот и детей, оставшихся без попечения родителей»»;

– Договоры, заключаемые между оператором и субъектом персональных данных;

– Согласия субъектов персональных данных на обработку персональных

данных;

– Устав муниципального образования Гусь-Хрустальный район Владимирской области, принят Решением Совета народных депутатов Гусь-Хрустального района от 28.06.2005 № 324.

6. Категории обрабатываемых субъектов персональных данных

6.1. В соответствии с целями обработки ПДн в администрации района осуществляется обработка следующих категорий субъектов ПДн:

– муниципальные служащие (работники);

– близкие родственники муниципальных служащих (родственники работников);

– уволенные муниципальные служащие (уволенные работники);

– руководители подведомственных учреждений;

– кандидаты на должность муниципальной службы (соискатели);

– физические лица, состоящие в договорных и иных гражданско-правовых отношениях (контрагенты);

– граждане, включенные в резерв управленческих кадров и граждане, претендующие на включение в резерв управленческих кадров;

– граждане, ПДн которых необходимы для выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей, оказания муниципальных услуг;

– граждане, ПДн которых необходимы для рассмотрения обращений граждан;

– посетители официального сайта администрации района;

– граждане, состоящие на учете в комиссии по делам несовершеннолетних и административной комиссии администрации района;

– законные представители.

6.2. Перечень и срок хранения обрабатываемых ПДн утверждается нормативным актом администрации района.

7. Порядок и условия обработки персональных данных

7.1. Принципы обработки ПДн

Обработка ПДн осуществляется администрацией района в соответствии со следующими принципами:

– обработка ПДн осуществляется на законной и справедливой основе;

– обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;

– не допускается обработка ПДн, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки; обрабатываемые ПДн не избыточны по отношению к заявленным целям их обработки;

– при обработке ПДн обеспечиваются точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн; Администрация района принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

– хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Пдн;

– обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7.2. Условия обработки персональных данных

Обработка ПДн сотрудников и граждан осуществляется с согласия на обработку ПДн.

7.2.1. Условия обработки специальных категорий персональных данных

Сведения, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни администрацией района не обрабатываются.

7.2.2. Условия обработки биометрических персональных данных

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются администрацией района для установления личности субъекта ПДн администрацией района не обрабатываются.

7.2.3. Условия обработки иных категорий персональных данных

Обработка иных категорий ПДн осуществляется администрацией района с соблюдением следующих условий:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

- обработка ПДн осуществляется в связи с участием лица в административном производстве;

- обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка ПДн необходима для исполнения полномочий в предоставлении государственных и муниципальных услуг, предусмотренных законодательством Российской Федерации.

- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом ПДн договор не может содержать положения, ограничивающие права и свободы субъекта ПДн, устанавливающие случаи обработки ПДн несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта ПДн.

7.2.4. Условия обработки общедоступных персональных данных

Обработка общедоступных ПДн в администрации района не осуществляется.

7.2.5. Поручение обработки персональных данных

7.2.5.1. Администрация района вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение).

7.2.5.2. Лицо, осуществляющее обработку ПДн по поручению администрации района, соблюдает принципы и правила обработки ПДн, предусмотренные настоящей Политикой. В поручении администрации района определяет перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, способы и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указаны требования к защите обрабатываемых ПДн.

7.2.5.3. При поручении обработки ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет администрация района. Лицо, осуществляющее обработку ПДн по поручению администрации района, несет ответственность перед администрацией района.

7.2.6. Передача персональных данных

7.2.6.1. Администрация района вправе передавать ПДн органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

7.3. Конфиденциальность персональных данных

7.3.1. Сотрудники администрации района, получившие доступ к ПДн, не раскрывают третьим лицам и не распространяют ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7.4. Общедоступные источники персональных данных

Администрация района не создает общедоступные источники ПДн.

7.5. Трансграничная передача персональных данных

7.5.1. Трансграничная передача ПДн администрацией района не осуществляется.

7.6. Обработка метаданных

7.6.1. На официальном сайте администрации района (gusr.ru) для качественного предоставления услуг применяется инструмент веб-аналитики Спутник-аналитика в целях анализа использования сайтов и улучшения их работы. Спутник-аналитика обрабатывает cookie - текстовые файлы, сохраняющиеся на компьютере пользователя и позволяющие анализировать посещение веб-сайтов. На официальном сайте администрации района отображается предупреждение, информирующее пользователей об обработке метаданных. При посещении официального сайта администрации района пользователь дает согласие администрации района на обработку указанных данных с использованием метрических сервисов для анализа использования, измерения и повышение уровня производительности официального сайта администрации района.

7.6.2. Обработка файлов cookie администрацией района осуществляется в обобщенном виде и никогда не соотносится с личными сведениями пользователей.

7.6.3. Согласие действует с момента его предоставления и в течение всего периода использования официального сайта администрации района пользователем.

7.6.4. В случае отказа от обработки файлов cookie пользователю необходимо прекратить использование официального сайта администрации района или отключить использование файлов cookie в настройках браузера, при этом некоторые функции официального сайта администрации района могут стать недоступны.

8. Согласие субъекта персональных данных на обработку его персональных данных

8.1. При необходимости обеспечения условий обработки ПДн субъекта может предоставляться согласие субъекта ПДн на обработку его ПДн.

8.2. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются администрацией района.

8.3. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн оператор вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии альтернативных условий обработки ПДн.

8.5.4. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство выполнения альтернативных условий обработки ПДн возлагается на администрацию района.

8.5.5. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении

согласия от представителя субъекта ПДн);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;

4) цель обработки ПДн;

5) перечень ПДн, на обработку которых дается согласие субъекта ПДн;

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

7) перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

8) срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта ПДн.

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

8.5.7. В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.

8.5.8. В случае смерти субъекта ДДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

8.5.9. ПДн могут быть получены администрацией района от лица, не являющегося субъектом ПДн, при условии предоставления администрации района подтверждения наличия альтернативных условий обработки информации.

9. Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов

9.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы администрации района подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

9.1.1. Законодательные (правовые) меры защиты.

К правовым мерам защиты относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоян-

ной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы администрации района.

9.1.2. Морально-этические меры защиты.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или администрации в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

9.1.3. Технологические меры защиты.

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

9.1.4. Организационные (административные) меры защиты.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

9.2. Формирование политики безопасности.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите ПДн) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в администрации района целесообразно разбить на два уровня. К верхнему уровню относятся решения, затрагивающие деятельность администрации в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн;

- кто имеет права доступа к ПДн, кто и при каких условиях может читать и

модифицировать ПДн и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

- определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

- выбирать программно-технические (аппаратные) средства противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

9.3. Регламентация доступа в помещения.

Компоненты ИСПДн администрации района должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, автоматизированных рабочих мест и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки ПДн в таких помещениях должен присутствовать только персонал, допущенный к работе с ПДн. Запрещается прием посетителей в помещениях, когда осуществляется обработка ПДн.

По окончании рабочего дня, помещения, в которых размещаются компоненты ИСПДн администрации района, должны запираться на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

9.4. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с ИСПДн администрации и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к ПДн, с которыми ему необходима работать в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информационной системы ПДн;

- глава администрации района имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники администрации района и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки ПДн, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению ПДн администрации района.

Обработка ПДн в компонентах ИСПДн администрации района должна производиться в соответствии с утвержденными технологическими инструкциями.

9.5. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников администрации района, с которых возможен доступ к ресурсам ИСПДн, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах ИСПДн и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

9.6. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационной системы, используемое для доступа и хранения ПДн, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

9.7. Подбор и подготовка персонала, обучение пользователей

Пользователи ИСПДн администрации района, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки ПДн в администрации района.

Обеспечение безопасности ПДн возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами администрации района. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи ИСПДн администрации района должны быть ознакомлены с организационно–распорядительными документами по обеспечению безопасности ПДн администрации района, в части, их касающейся, должны знать и неу-

коснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых ПДн, должно осуществляться под роспись.

9.8. Ответственность за нарушения установленного порядка пользования ресурсами ИСПДн администрации района.

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с ПДн, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению главы администрации района.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

9.9. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности администрации района используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационной системы администрации района, независимо от их вида и формы представления информации в них.

9.9.1. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым ПДн, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов ИСПДн администрации района необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки ПДн, на:

- наличие специально внедренных закладных устройств;
- введение дополнительных ограничений по доступу в помещения, предна-

значенные для хранения и обработки ПДн;

- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

9.9.2. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;
- средства регистрации доступа к компонентам ИСПДн и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

9.9.3. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами ИСПДн администрации района посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;
- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

9.9.4. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты

устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к компонентам информационной среды администрации района и элементам системы защиты ПДн (физический доступ);
- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.);
- к операционной системе, системным программам и программам защиты.

9.9.5. Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

9.9.6. Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта, осуществляющего регистрируемое действие;
- действие (тип доступа).

9.10. Контроль эффективности системы защиты

Контроль эффективности защиты ПДн осуществляется с целью своевременного выявления и предотвращения утечки ПДн за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

10. Порядок доступа субъекта персональных данных к его персональным данным

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

10.2. Сведения должны быть предоставлены субъекту ПДн администрацией района в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

10.3. Сведения предоставляются субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с администрацией района либо сведения, иным образом подтверждающие факт обработки ПДн администрацией района, подпись субъекта ПДн или его представителя.

10.4. Администрация района вправе отказать субъекту ПДн в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на администрации района.

10.5. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн администрацией; правовые основания и цели обработки Пдн;
- цели и применяемые администрацией способы обработки ПДн;
- наименование и место нахождения администрации, сведения о лицах, ко-

торые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с администрацией района или на основании федерального закона;

- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки ПДн, в том числе сроки их хранения;

- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению администрации, если обработка поручена или будет поручена такому лицу.

10.6. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

11. Обязанности администрации района

11.1. Администрация обязана безвозмездно предоставить субъекту ПДн его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, администрация района обязана внести в них необходимые изменения.

11.2. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн администрация района обязана осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению администрации) с момента такого обращения или получения указанного запроса на период проверки.

11.3. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн администрация района обязана осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению администрации) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

11.4. В случае подтверждения факта неточности ПДн администрация района на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязана уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению администрации) в течение семи рабочих дней со дня представления таких сведений и

снять блокирование ПДн.

11.5. В случае выявления неправомерной обработки ПДн, осуществляемой администрацией района или лицом, действующим по поручению администрации района, администрация района в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению администрации района.

11.6. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», администрация района обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации, обрабатываемых в следующих информационных системах:

- ИСПДн «Сотрудники» с использованием баз данных, находящихся на территории России.
- ИСПДн«Обращения граждан» с использованием баз данных, находящихся на территории России.
- ИСПДн«СМЭВ» с использованием баз данных, находящихся на территории России.

Местонахождение центра(ов) обработки данных и сведения об организации, ответственной за хранение данных, определены внутренними документами администрации района.

12. Условия прекращения обработки персональных данных

12.1. Обработка ПДн ограничивается достижением конкретных, заранее определённых и законных целей.

12.2. Обработка ПДн субъекта ПДн прекращается в случае ликвидации оператора, реорганизации оператора, прекращения деятельности по обработке ПДн, наступления срока (условия) прекращения обработки ПДн, указанного в уведомлении, вступившего в законную силу решение суда, или иных оснований. Субъектом ПДн и оператором подписывается уведомление о прекращении обработки ПДн, в соответствии с утвержденной формой.

12.3. Сроки хранения документов, содержащих ПДн субъектов, определяются в соответствии со сроком действия договора с субъектом ПДн, Федеральным законом РФ от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения"».

12.4. Порядок уничтожения носителей содержащих ПДн определяется в соответствии с Положением Об уничтожении ПДн, обрабатываемых в администрации района.

13. Ответственность

13.1. Лица, виновные в нарушении требований Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

13.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

14. Ключевые результаты

При достижении целей ожидаются следующие результаты:

– обеспечение защиты прав и свобод субъектов пПДн при обработке его ПДн администрацией района;

– повышение общего уровня информационной безопасности администрации района;

– минимизация юридических рисков администрации района.