**РАСПОРЯЖЕНИЕ**

ГЛАВЫ АДМИНИСТРАЦИИ МЕСТНОГО

САМОУПРАВЛЕНИЯ МОЗДОКСКОГО РАЙОНА

РЕСПУБЛИКИ СЕВЕРНАЯ ОСЕТИЯ-АЛАНИЯ

№1014 г. Моздок

23.08.2023 г.

*О защите информации в Администрации местного*

*самоуправления Моздокского района*

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Главы Администрации местного самоуправления Моздокского района от 26.12.2022 №163-Д «Об изменении структуры и штатов Администрации местного самоуправления Моздокского района»:

1. Возложить обязанности по защите информации:
   1. Назначить ответственным за организацию обработки персональных данных, обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) главного специалиста по информатизации отдела информационных технологий, защиты информации и муниципальных услуг Администрации местного самоуправления Моздокского района - Мещерякова Николая Александровича.
   2. Назначить ответственным за эксплуатацию программных продуктов (информационных систем персональных данных, при их наличии) ведущего специалиста – программиста отдела информационных технологий, защиты информации и муниципальных услуг Администрации местного самоуправления Моздокского района – Мысикова Егора Владимировича.
   3. Назначить ответственным за ведение журналов по защите информации главного специалиста по информатизации отдела информационных технологий, защиты информации и муниципальных услуг Администрации местного самоуправления Моздокского района - Мещерякова Николая Александровича.

2.Утвердить:

2.1.Положение о порядке обработки персональных данных без использования средств автоматизации в Администрации местного самоуправления Моздокского района, согласно [приложению №1](#Пр5) к настоящему распоряжению.

2.2. Положение об обработке персональных данных с использованием средств автоматизации в Администрации местного самоуправления Моздокского района, согласно [приложению №2](#Пр5) к настоящему распоряжению.

2.3. Положение об организации режима обеспечения безопасности помещений Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, в которых ведется обработка персональных данных, согласно приложения №[3](#Пр5) к настоящему распоряжению.

2.4. Регламент по резервному копированию и восстановлению данных Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, согласно [приложению №4](#Пр21) к настоящему распоряжению.

2.5. Инструкцию ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, согласно приложению №5 к настоящему распоряжению.

2.6. Инструкцию по организации антивирусной защиты в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, согласно приложению №6 к настоящему распоряжению.

2.7. Инструкцию по организации парольной защиты в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, согласно приложению №7 к настоящему распоряжению.

2.8. Инструкцию пользователя программных продуктов (информационных систем персональных данных, при их наличии) в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания согласно приложение №8 к настоящему распоряжению.

2.9. Порядок уничтожения персональных данных в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, согласно [приложению №9](#Пр26) к настоящему распоряжению.

2.10. Правила рассмотрения запросов субъектов персональных данных или их представителей в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания Алания, согласно [приложению №10](#Пр26) к настоящему распоряжению.

3.Утвердить формы журналов по защите информации, согласно [приложению №11](#Пр26) к настоящему распоряжению.

4. Признать утратившими силу приложения №1, №3, №4, №5, №6, №7, №8, №9, №10, №11, №12, №13, №14, №15, №16, №17, №18, №19, №20, №21, №22 к распоряжению Главы Администрации местного самоуправления Моздокского района от 17.11.2020 №924 «О защите информации».

5. Настоящее распоряжение вступает в силу со дня его официального опубликования.

6. Отделу информационных технологий, защите информации и муниципальных услуг Администрации местного самоуправления Моздокского района опубликовать настоящее распоряжение в печатном периодическом издании «Время, события, документы» и разместить на официальном сайте Администрации местного самоуправления Моздокского района в информационно-телекоммуникационной сети «Интернет» admmozdok.ru.

7. Главному специалисту - юрисконсульту отдела по **юридическим вопросам, кадровой политики и профилактики коррупционных правонарушений** Администрации местного самоуправления Моздокского района направить настоящее распоряжение в Администрацию Главы Республики Северная Осетия-Алания и Правительства Республики Северная Осетия-Алания с помощью соответствующего программного обеспечения – программного продукта «АРМ Муниципал».

8. Контроль за исполнением настоящего распоряжения возложить на начальника отдела информационных технологий, защите информации и муниципальных услуг Администрации местного самоуправления Моздокского района.

Глава Администрации Р. Адырхаев

Исп. И. Заварзина, тел.: 3-47-85

*Приложение № 1*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ПОЛОЖЕНИЕ

о порядке обработки персональных данных без использования средств автоматизации в Администрации местного самоуправления Моздокского района

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Правила обработки персональных данных, осуществляемой без использования средств автоматизации в Администрации местного самоуправления Моздокского района (далее – Администрация), установленные настоящим Положением, должны применяться с учетом требований постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687.
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ
   1. Контролируемая зона (КЗ) – это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
   2. Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
   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. Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
   5. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных.
   6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
   7. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.
   8. 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.
3. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ

АВТОМАТИЗАЦИИ

* 1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).
  2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
  3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Администрации или лица, осуществляющие такую обработку по договору с Администрацией), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Администрацией без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Республики Северная Осетия-Алания, а также локальными правовыми актами Администрацией.
  4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:
     1. типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Администрации, 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 Администрацией способов обработки персональных данных;
     2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации (при необходимости получения письменного согласия на обработку персональных данных);
     3. 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.
  5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение Администрации или в иных аналогичных целях, должны соблюдаться следующие условия:
     1. необходимость ведения такого журнала должна быть предусмотрена нормативно-правовым актом Администрацией, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;
     2. копирование содержащейся в таких журналах информации не

допускается;

* + 1. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных.
  1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).
  2. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта.
  3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

1. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ
   1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
   2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
   3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются нормативно-правовым актом Администрации.
2. ОТВЕТСТВЕННОСТЬ
   1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей информационных систем, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных Администрации.
   2. Работники персональных данных Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.
      1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).
      2. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.
      3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.
   3. Глава Администрации, заместители Главы Администрации, руководители структурных подразделений Администрации за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

*Приложение № 2*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ПОЛОЖЕНИЕ

об обработке персональных данных с использованием средств автоматизации в Администрации местного самоуправления Моздокского района

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации (далее – Положение) Администрации местного самоуправления Моздокского района (далее – Администрация), разработано в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации и Республики Северная Осетия-Алания.

1.2. Цели разработки Положения:

1.2.1. Определение порядка обработки персональных данных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Администрации;

1.2.2. Обеспечение защиты прав и свобод человека и гражданина при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. Установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

- обезличенных персональных данных;

- общедоступных персональных данных.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии Администрации, если иное не определено законом Российской Федерации.

II.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

* 1. Доступ к информации – возможность получения информации и ее использования.
  2. Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.
  3. Информация – сведения (сообщения, данные) независимо от формы их представления.
  4. Контролируемая зона (КЗ) – это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
  5. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
  6. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
  7. 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.
  8. 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.
  9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
  10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
  11. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

III.ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Обработка персональных данных может осуществляться исключительно в целях, указанных в Политики Администрации местного самоуправления Моздокского района в отношении обработки персональных данных.

При определении объема и содержания, обрабатываемых персональных данных работники Администрации должны руководствоваться Политикой Администрации местного самоуправления Моздокского района в отношении обработки персональных данных с учетом действующего законодательства Российской Федерации, а также настоящим Положением.

3.2. Обработка персональных данных с использованием средств автоматизации (автоматизированным способом) может осуществляться исключительно на автоматизированных рабочих местах ИСПДн, утверждённых Перечнем автоматизированных рабочих мест, использующих программные продукты для обработки персональных данных, согласно приложению №1 к настоящему положению.

3.3. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в Администрации определяется Политикой Администрации местного самоуправления Моздокского района в отношении обработки персональных данных.

IV.ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Хранение носителей (дискет, дисков, флеш-накопителей и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

4.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.3. Обработка персональных данных в Администрации осуществляется до наступления одного из условий прекращения обработки персональных данных, указанных в Политике Администрации местного самоуправления Моздокского района в отношении обработки персональных данных.

По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

Обезличивания персональных данных в Администрации не предполагается.

V.ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Передавать персональные данные субъектов допускается только тем работникам, которые имеют допуск к обработке персональных данных.

В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Администрация в ходе своей деятельности предоставляет персональные данные организациям, перечисленным в Политике Администрации местного самоуправления Моздокского района в отношении обработки персональных данных.

5.2. Не допускается распространение персональных данных субъекта.

VI.ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Администрация за счет своих средств.

6.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

6.2.1. Проведение организационных мероприятий:

а) разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

б) ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

в) организация учёта носителей персональных данных;

г) разработка модели угроз безопасности персональным данным;

д) проведение обучения работников по вопросам защиты персональных данных.

6.2.2. Программно-аппаратная защита:

а) внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом № 184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия.

6.2.3. Инженерно-техническая защита:

а) установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

б) установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

6.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Администрации.

Организацию и контроль защиты персональных данных в структурных подразделениях Администрации осуществляют их непосредственные руководители.

VII.ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Допуск к персональным данным субъекта могут иметь только те работники Администрации, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей» согласно приложению №2 к настоящему положению.

7.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

7.2.1. Ознакомление работника с настоящим Положением, Политикой Администрации местного самоуправления Моздокского района в отношении обработки персональных данных и другими локальными нормативно-правовыми актами Администрации, касающимися обработки персональных данных;

7.2.2. Истребование с работника Обязательства о неразглашении информации ограниченного доступа.

7.3. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

7.4. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

VIII.ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

8.1. Состав информационных систем Администрации определяется Перечнем информационных систем, согласно приложению 3 к настоящему положению.

8.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

8.3. 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.

8.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

8.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

8.6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.7. Безопасность персональных данных при их обработке в информационной системе обеспечивает специалист, ответственный за обеспечение безопасности персональных данных в информационных системах.

8.8. При обработке персональных данных в информационной системе должно быть обеспечено:

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

б) Своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) Постоянный контроль над обеспечением уровня защищенности персональных данных.

8.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

8.9.1. Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

8.9.2. Разработку на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

8.9.3. Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

8.9.4. Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

8.9.5. Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

8.9.6. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

8.9.7. Учет лиц, допущенных к работе с персональными данными в информационной системе;

8.9.8. Контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

8.9.9. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

8.9.10. Описание системы защиты персональных данных.

8.9.11. Иные требования по обеспечению безопасности информации и средств защиты информации в Администрации в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Республики Северная Осетия-Алания.

IX.ОТВЕТСТВЕННОСТЬ

9.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных в Администрации.

9.2. Работники Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

9.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба (в соответствии с п.7 ст. 243 Трудового кодекса Российской Федерации).

9.4. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях Российской Федерации.

9.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса Российской Федерации.

9.6. ГлаваАдминистрации, заместители Главы Администрации, руководители структурных подразделений Администрации, за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

*Приложение № 1 к*

*Положению об обработке персональных данных с использованием средств автоматизации в Администрации местного самоуправления Моздокского района*

ПЕРЕЧЕНЬ

автоматизированных рабочих мест, использующих программные продукты для обработки персональных данных

| № п/п | Наименование | Допущенные лица | Месторасположение | Наименование ИС |
| --- | --- | --- | --- | --- |
|  | АРМ начальника **отдела бухгалтерского учета и осуществления закупок для муниципальных нужд** | начальник **отдела бухгалтерского учета и осуществления закупок для муниципальных нужд** | Кабинет №10 | 1С-бухгалтерия |
|  | АРМ заместитель начальника **отдела бухгалтерского учета и осуществления закупок для муниципальных нужд** | заместитель начальника **отдела бухгалтерского учета и осуществления закупок для муниципальных нужд** | Кабинет №10 | 1С-бухгалтерия |
|  | АРМ Консультант по кадровым вопросам **отдела по юридическим вопросам, кадровой политики и профилактики коррупционных правонарушений** | консультант по кадровым вопросам **отдела по юридическим вопросам, кадровой политики и профилактики коррупционных правонарушений** | Кабинет №16 | 1С-Кадры |

*Приложение № 2 к*

*Положению об обработке персональных данных с использованием средств автоматизации в Администрации местного самоуправления Моздокского района*

Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей

|  |  |
| --- | --- |
| № п/п | Наименование должности |
| Доступ персональных данных сотрудников Администрации | |
| 1 | Глава Администрации |
| 2 | Первый заместитель Главы Администрации (к персональным данным сотрудников курируемых подразделений) |
| 3 | Заместители Главы Администрации (к персональным данным сотрудников курируемых подразделений) |
| 4 | **Специалисты отдела по юридическим вопросам, кадровой политики и профилактики коррупционных правонарушений** |
| 5 | **Специалисты отдела бухгалтерского учета и осуществления закупок для муниципальных нужд** |
| 6 | **Специалисты мобилизационного отдела** |
| 7 | **Специалисты отдела по организационным и общим вопросам** |
| 8 | **Специалисты отдела информационных технологий, защиты информации и муниципальных услуг** |
| Доступ к персональным данным граждан, обращающимся в Администрацию | |
| 1 | Глава Администрации |
| 2 | Первый заместитель Главы Администрации |
| 3 | Заместители Главы Администрации |
| 4 | Руководители и специалисты структурных подразделений, в целях исполнения должностных обязанностей |

*Приложение № 3*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ПОЛОЖЕНИЕ

об организации режима обеспечения безопасности помещений Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, в которых ведется обработка персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Под контролируемой зоной (далее – КЗ) понимается территория, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.
   2. Схемы контролируемой зоны фиксируются в технических паспортах на информационные системы. Администратор информационной безопасности обеспечивает актуальность приведенной в технических паспортах информации.
   3. Охраной помещений во внерабочее время занимается штатный охранник.
2. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ
   1. Помещения, в которых осуществляется обработка персональных данных, должны быть оборудованы охранной и пожарной сигнализациями, а также прочными дверьми с механическими замками.
   2. Ключи от помещений выдаются и находятся на ответственном хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей.
   3. Сотрудникам, которым необходим временный доступ в помещения, к которым у них нет допуска, может быть предоставлен такой доступ, но только в присутствии сотрудников, работающих в этом помещении (имеющих доступ в это помещение).
   4. При покидании помещения и при отсутствии в нем других лиц, допущенных в это помещение, сотрудник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.
   5. Перед началом рабочего дня помещения снимаются с охраны. После окончания рабочего дня, помещения устанавливаются под охрану в соответствии с установленным в разделе 3 настоящего положения порядком.
   6. Нахождение посторонних лиц в помещениях, в которых осуществляется обработка персональных данных, допускается только в присутствии сотрудников, работающих в данном помещении и при условии соблюдения правил ограничения доступа к обрабатываемой информации.

3. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

* 1. Закрытие помещений, в которых обрабатываются персональные данные, осуществляется по окончании рабочего дня последним сотрудником, покидающим помещение. Закрытие помещения осуществляется после проведения в нем уборки, обесточивания оборудования, запирания сейфов, закрытия окон.
  2. После запирания помещения на ключ, установки охранной сигнализации и сдачи ключа от помещения под роспись, помещение считается принятым под охрану.
  3. При вскрытии помещения, допущенные в него сотрудники осуществляют осмотр на предмет выявления признаков несанкционированных действий в помещении в их отсутствие (повреждения дверей, повреждения пломб, изменение местоположения мебели, включенная техника и т. п.). При отсутствии нарушений, помещение считается снятым с охраны.
  4. В случае обнаружения нарушений, сотрудник сообщает об этом ответственному за организацию обработки персональных данных.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

* 1. Настоящее положение может быть изменено и дополнено по следующим причинам:
* появление информации о новых угрозах безопасности информации, связанных с физическим доступом к техническим средствам информационных систем;
* при возникновении инцидентов информационной безопасности, связанных с физическим доступом, извлечения из них уроков и понимания необходимости пересмотра настоящего положения;
* при изменении законодательства в сфере защиты информации.
  1. За нарушение настоящего положения, сотрудники могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.

*Приложение № 4*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

РЕГЛАМЕНТ

по резервному копированию и восстановлению данных Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

I ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Настоящий Регламент резервного копирования и восстановления данных, хранящихся на сервере и автоматизированных рабочих местах Администрации (далее - Регламент) разработан в соответствии с требованиями Федерального Закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ, приказа ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г. № 21, приказа ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» № 17 от 11.02.2013 г.
  2. Настоящий Регламент разработан с целью:
     1. Определения порядка резервирования данных для последующего восстановления работоспособности программных продуктов, хранящихся на сервере Администрации при полной или частичной потере информации, вызванной попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
     2. Определения порядка восстановления информации в случае возникновения такой необходимости.
  3. В настоящем документе регламентируются действия при выполнении следующих мероприятий:
     1. резервное копирование;
     2. контроль резервного копирования;
     3. хранение резервных копий;
     4. полное или частичное восстановление данных и приложений.
  4. Если резервирование предполагает выгрузку на съемные носители информации, то такие носители должны учитываться в порядке, установленном «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах».

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ
   1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.
   2. Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)
   3. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
   4. Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)
   5. Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.
   6. Система резервного копирования – совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.
2. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ
   1. Резервному копированию подлежит информация следующих основных категорий:
      1. данные (файлы и каталоги) на файловых серверах;
      2. базы данных;
   2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.
   3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено ответственному за организацию обработки персональных Администрации.
   4. Для организации системы резервного копирования используются стандартные средства Windows.
   5. Существуют следующие наборы резервных копий:
      1. месячный набор - записывается информация на первое число текущего месяца. Срок хранения – 1 (один) месяц;
      2. недельная копия - записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы;
      3. суточная копия - записывается ежедневно в 12:00. Срок хранения - сутки.
   6. Копии хранятся на сервере резервного копирования.
   7. Для резервирования информации, хранимой непосредственно в файловых системах, используются стандартные средства Windows.
   8. Для резервирования информации, хранимой в базах данных сервера Администрации, в качестве промежуточного звена автоматизации используются средства конфигурирования и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных. Посредством стандартных средств Windows формируются задания на проведение резервного копирования этого каталога.
3. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ
   1. Контроль результатов всех процедур резервного копирования осуществляется ответственным за обеспечение безопасности персональных данных в Администрации.
   2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.
4. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ
   1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются ответственным за обеспечение безопасности персональных данных в Администрации. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.
   2. Носители с защищаемой информацией, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.
5. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНОЙ КОПИИ
   1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя программного продукта. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более 1 (одного) рабочего дня.
   2. Любое восстановление информации выполняется на основании заявки пользователя ответственному за обеспечение безопасности персональных данных в Администрации или в случае необходимости восстановления утерянной или повреждённой информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, на систему резервного копирования программного обеспечения.

*Приложение № 5*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах

(информационных системах персональных данных, при их наличии)

в Администрации местного самоуправления Моздокского района

Республики Северная Осетия-Алания

I ОБЩИЕ ПОЛОЖЕНИЯ

1. Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) Администрации местного самоуправления Моздокского района (далее – Администрация).

1.2. Решение вопросов организации защиты обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) в Администрации входит в прямые служебные обязанности главного специалиста по информатизации отдела информационных технологий, защиты информации и муниципальных услуг Администрации.

1.3. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) обладает правами доступа к любым носителям персональных данных и в любое помещение, где осуществляется обработка персональных данных Администрации.

II ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
2. Доступ к информации – возможность получения информации и её использования.
3. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
4. Контролируемая зона (КЗ) – это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
5. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, электронных и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.
6. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
7. 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.
8. Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.
9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
10. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.
11. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

3. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) обязан:

1. Знать перечень и условия обработки персональных данных в Администрации.

3.2. Знать и предоставлять изменения на утверждение Главе Администрации в Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей программных продуктах (информационных системах персональных данных, при их наличии), оформлении разрешительной системы доступа, минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в порядке, установленном главой IV настоящей Инструкции.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. Производить периодический контроль за соблюдением режима безопасности помещений, в которых осуществляется обработка персональных данных, путем:

3.8.1. контроля процесса доступа и нахождения в помещении лиц, не имеющим права доступа к персональным данным;

3.8.2. контроля исключения доступа к персональным данным лиц, не имеющим права доступа к персональным данным;

3.8.3. контроля обеспечения сохранности персональных данных, в т.ч. хранилищ и носителей персональных данных.

3.9. Производить периодический контроль за соблюдением режима безопасности помещений, в которых размещена информационная система, путем:

3.9.1. контроля обеспечения сохранности и работоспособности технических средств информационной системы;

3.9.2. контроля расположения мониторов для исключения несанкционированного просмотра возможным внешним нарушителем;

3.9.3. контроля исключения несанкционированного просмотра при обработке персональных данных.

3.10. Поддерживать в актуальном состоянии локальные документы, направленные на обеспечение защиты персональных данных.

3.11. Своевременно и точно вносить изменения в локальные нормативно-правовые акты по правилам обработки и защиты персональных данных. 3.12. Проводить с работниками и руководителями структурных подразделений занятия по изучению руководящих документов в области обеспечения безопасности персональных данных и инструктажи о порядке работы с персональными данными.

3.13. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.14. Контролировать соблюдение работниками локальных документов, регламентирующих порядок работы с программными, техническими средствами и персональными данными.

3.15. Вносить свои предложения по совершенствованию мер защиты персональных данных, разработке и принятию мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.16. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов в установленные законодательством сроки.

3.17. Представлять интересы Администрации при проверках надзорных органов в сфере обработки персональных данных.

3.18. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

* 1. К попыткам несанкционированного доступа относятся:
     1. Сеансы работы с персональными данными незарегистрированными пользователями, или пользователями, нарушившими установленную периодичность доступа, срок действия полномочий которых истёк или превышающих свои полномочия по доступу к данным;
     2. Действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к программным продуктам (информационным системам персональных данных, при их наличии), при использовании учётной записи администратора или другого пользователя методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.
  2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) обязан:
     1. Прекратить несанкционированный доступ к персональным данным;
     2. Доложить Главе Администрации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
     3. Известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;
     4. Известить администратора безопасности в программных продуктах (информационных системах персональных данных, при их наличии) о факте несанкционированного доступа.

V ПРАВА

5. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) имеет право:

* 1. Требовать от работников выполнения локальных нормативно-правовых актов в части работы с персональными данными.
  2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.
  3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами в программных продуктах (информационных системах персональных данных, при их наличии), в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI ОТВЕТСТВЕННОСТЬ

6.1. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в программных продуктах (информационных системах персональных данных, при их наличии), если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

6.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

6.4. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

6.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни) предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

С инструкцией ознакомлен (а): подпись ФИО

*Приложение № 6*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ИНСТРУКЦИЯ

по организации антивирусной защиты в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

I ОБОБЩИЕ ПОЛОЖЕНИЯ

1. Данная инструкция определяет требования к организации в программных продуктах (информационных системах, при их наличии) Администрации от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность пользователей в программных продуктах (информационных системах, при их наличии) Администрации, за выполнение указанных требований.

II ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Антивирусная база – это база, которая содержит уникальные данные о каждом конкретном вирусе

2.2. Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.3. Средство антивирусной защиты – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

2.4. Автоматизированное рабочее место (АРМ) – это рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций.

2.5. Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

2.6. Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.7. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации

2.8. Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)

2.9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

III ОБЯЗАННОСТИ

3.1. К использованию в Администрации допускаются только сертифицированные и лицензионные средства антивирусной защиты, закупленные у разработчиков или поставщиков данных средств отраженные в «Журнале учета средств защиты информации, эксплуатационной и технической документации к ним в Администрации».

3.2. Установка средств антивирусного контроля на автоматизированных рабочих местах в Администрации осуществляется ответственным за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии) или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты информации.

3.3. Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.

3.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

3.5. Процедура обновления баз средства антивирусной защиты должна проводиться в автоматическом режиме не реже 1 (одного) раза в неделю для всех АРМ.

3.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено ответственным за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии) (далее – ПО).

3.7. Подключаемые к компьютеру внешние устройства и носители информации должны проверяться антивирусным ПО непосредственно после подключения.

3.8. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в Администрации, осуществляется ответственным за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии).

IV ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с ответственным за эксплуатацию программных продуктов (информационных систем персональных данных, при их наличии) провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах ответственного за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии) для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

4.2.1. приостановить обработку данных;

4.2.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения ответственного за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии), владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

4.2.3. совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

4.2.4. произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за эксплуатацию программных продуктах (информационных систем персональных данных, при их наличии).

V ОТВЕТСТВЕННОСТЬ

5.1. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени их учётных записей в программных продуктах (информационных систем персональных данных, при их наличии), если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.4. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

5.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

*Приложение № 7*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ИНСТРУКЦИЯ

по организации парольной защиты в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

I ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в Администрации, а также контроль над действиями пользователей при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех программных продуктах (информационных системах, при наличии) и контроль за действиями пользователей при работе с паролями возлагается на ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии).

II ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.2. Информационная система (ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.5. Компрометация пароля – раскрытие, обнаружение или утеря пароля.

III ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫ В ПРОГРАММНЫХ ПРОДУКТАХ (ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ,

ПРИ ИХ НАЛИЧИИ)

3.1.Правила формирования паролей:

3.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями программных продуктов (информационных системах персональных данных, при их наличии) самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);

- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;

3.1.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.1.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии).

3.2. Порядок смены личных паролей:

3.2.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

3.2.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя.

3.2.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии), администраторов и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.2.4. Ответственный за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) ведёт Журнал учёта работ в программных продуктах (информационных системах персональных данных, при их наличии), в котором он отмечает факт смены паролей пользователей.

3.2.5. Временный пароль, заданный ответственным за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

3.3. Действия в случае утери и компрометации пароля:

3.3.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ПРОГРАММНЫХ ПРОДУКТОВ (ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ,

ПРИ ИХ НАЛИЧИИ)

4.1. Правила формирования паролей:

4.1.1. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);

- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

4.1.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

4.1.3. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) в запечатанном конверте или опечатанном пенале.

4.2. Порядок Ввод пароля:

4.2.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.3. Порядок смены личных паролей:

4.3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем;

4.3.2. Временный пароль, заданный ответственным за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

4.4. Хранение пароля:

4.4.1. запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации;

4.4.2. запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей;

4.4.3. запрещается регистрировать других пользователей в программных продуктах (информационных системах персональных данных, при их наличии) со своим личным паролем, запрещается входить в программные продукте (информационные системы персональных данных, при их наличии) под учётной записью и паролем другого пользователя.

4.5. Действия в случае утери и компрометации пароля:

4.5.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) с целью смены личного пароля.

V ОТВЕТСТВЕННОСТЬ

5.1. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в программных продуктах (информационных системах персональных данных, при их наличии), если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение информации (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.4. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

5.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

*Приложение № 8*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ИНСТРУКЦИЯ

пользователя программных продуктов (информационных систем персональных данных, при их наличии) в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

I ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Настоящая инструкция регламентирует обязанности работников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программным продуктам (информационным системам персональных данных, при их наличии) в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания.

1. Термины и определения
   1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.
   2. База данных – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры
   3. Информация – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).
   4. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).
   5. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
   6. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).
   7. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.
   8. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).
   9. Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации (ISO/IEC 2382-1:1993)
   10. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).
   11. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
2. Общие обязанности работников

Каждый работник Администрации, являющийся пользователем программных продуктов (информационных систем персональных данных, при их наличии), обязан:

* 1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными продуктами (информационными системами персональных данных, при их наличии).
  2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его АРМ.
  3. Соблюдать правила работы с паролем своей учётной записи.
  4. Немедленно вызывать ответственного за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) и поставить в известность руководителя структурного подразделения при обнаружении:
     1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;
     2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
     3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
     4. некорректного функционирования установленных на АРМ технических средств защиты;
     5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.
  5. Всем работникам Администрации, являющимся пользователями программных продуктах (информационных системах персональных данных, при их наличии), запрещается:
     1. использовать компоненты программного и аппаратного обеспечения Администрации в неслужебных целях;
     2. самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии);
     3. оставлять без присмотра своё АРМ не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы;
     4. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

1. ОБЕСПЕЧеНИЕ СОХРАННОСТИ ИНФОРМАЦИИ
   1. Для обеспечения программных продуктов (информационных систем персональных данных, при их наличии) необходимо соблюдать следующие требования:
      1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.
   2. Субъектам доступа запрещается:
      1. Установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети.
      2. Самовольное изменение сетевых адресов.
      3. Самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения.
      4. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за организацию обработки персональных данных и обеспечение безопасности персональных данных в программных продуктах (информационных системах персональных данных, при их наличии) с предварительно удаленными сетевыми настройками.
   3. Сведения, содержащиеся в электронных документах и базах данных Администрации, должны использоваться только в служебных целях в рамках полномочий работника, работающего с соответствующими материалами.
2. Ответственность за нарушение правил работы
   1. Каждый пользователь программных продуктов (информационных систем персональных данных, при их наличии) несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в программных продуктах (информационных системах персональных данных, при их наличии), если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.
   2. За разглашение персональных данных и нарушение порядка работы с программными продуктами (информационными системами персональных данных, при их наличии), содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.
   3. Распространение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами Администрации, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Администрации, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации (в соответствии с п.7 ст. 243 Трудового кодекса РФ). В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.
   4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

*Приложение № 9*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ПОРЯДОК

уничтожения персональных данных в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящий Порядок определяет условия и способы уничтожения персональных данных, содержащихся на бумажных и машинных носителях информации Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания (далее - Администрация).
2. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
   1. Администрация в случае выявления их неправомерной обработки и отсутствия возможности ее обеспечить в срок не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных или в случае достижения цели обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение.
   2. Уничтожение носителей персональных данных осуществляется комиссией. Комиссию возглавляет ответственный за организацию обработки персональных данных в Администрации. Уничтожение должно происходить в присутствии всех членов комиссии:
      1. уничтожение бумажных носителей осуществляется путем сожжения, измельчения или их химического разложения;
      2. уничтожение электронных файлов, содержащих персональные данные осуществляется путем их удаления с использованием средствами операционной системы с последующим «очищением корзины». Допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete»);
      3. уничтожение машинных носителей, содержащих персональные данные, осуществляется путем деформирования, нарушения единой целостности носителя или его сожжения.
   3. Факт уничтожения машинных носителей фиксируется комиссией в Акте уничтожения носителей и «Журнале учета съемных машинных носителей персональных данных в Администрации», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные.
   4. Об устранении допущенных нарушений или об уничтожении персональных данных Администрация уведомляет субъект персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

*Приложение № 10*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ПРАВИЛА

рассмотрения запросов субъектов персональных данных или

их представителей в Администрации местного самоуправления

Моздокского района Республики Северная Осетия-Алания

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания (далее – Администрация) определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).
2. Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 № 152 ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 2 мая 2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (в редакции от 29.06.2010 № 126-ФЗ, от 27.07.2010 № 227-ФЗ), Федеральным законом от 27 июля 2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 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» и другими нормативными правовыми актами.
3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных ([часть 7](#sub_1404) статьи 14 Федерального закона), в том числе содержащей:
   * подтверждение факта обработки персональных данных в Администрации;
   * правовые основания и цели обработки персональных данных;
   * цели и применяемые в Администрации способы обработки персональных данных;
   * наименование и место нахождения Администрации, сведения о лицах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федерального закона;
   * обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
   * сроки обработки персональных данных, в том числе сроки их хранения;
   * порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
   * информацию об осуществленной или о предполагаемой трансграничной передаче данных;
   * наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению руководителя, если обработка поручена или будет поручена такому лицу;
   * иные сведения, предусмотренные Федеральным законом или другими федеральными законами.
4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с [частью 8](#sub_1405) статьи 14 Федерального закона.
5. Субъект персональных данных вправе требовать от Администрации 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.
6. Сведения, указанные в [части 7](#sub_1404) статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
7. Сведения, указанные в [части 7](#sub_1404) статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю Администрацией при обращении либо при получении запроса субъекта персональных данных или его представителя.
8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Администрацией (номер заявки на возврат, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Администрацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан [электронной подписью](garantF1://12084522.21) в соответствии с законодательством Российской Федерации.
9. Рассмотрение запросов является служебной обязанностью уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.
10. Должностные лица Администрации обеспечивают:
    * объективное, всестороннее и своевременное рассмотрения запроса;
    * принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
    * направление письменных ответов по существу запроса.
11. Ведение делопроизводства по запросам осуществляется назначенным сотрудником Администрации.
12. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.
13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в [части 7](#sub_1404) статьи 14 Федерального закона №152-ФЗ, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения сведений, указанных в [части 7](#sub_1404) статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в Администрацию или направить повторный запрос в целях получения сведений, указанных в [части 7](#sub_1404) статьи 14 Федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

1. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [частями 4](#sub_1404) и [5](#sub_1405) статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным.
2. Прошедшие регистрацию запросы в тот же день докладываются Главе Администрации, либо лицу его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.
3. Глава Администрации и другие должностные лица при рассмотрении и разрешении запроса обязаны:
   * внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;
   * принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
   * сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.
4. Ответственные лица Администрации обязаны сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.
5. 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 их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица Администрации обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение [части 8 статьи 14](#sub_1405) 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.
6. Администрация обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.
7. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица Администрации обязаны внести в них необходимые изменения.
8. 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, уполномоченные должностные лица Администрации обязаны уничтожить такие персональные данные.
9. Администрация обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Администрации обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.
11. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Администрации обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.
12. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Администрации на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.
13. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Администрации в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица Администрации в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Администрация обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
14. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.
15. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками Администрации действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются Главе Администрации.
16. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.
17. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.
18. Глава Администрации осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.
19. Глава Администрации осуществляет контроль за работой с запросами и организацией их приема как лично, так и через своих заместителей. На контроль берутся все запросы.
20. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.
21. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Сводная таблица действий в ответ на запросы по персональным данным

| № | Запрос | Действия | Срок | Ответ |
| --- | --- | --- | --- | --- |
| I. Запрос Субъекта ПДн или его Представителя | | | | |
| 1.1. | Наличие ПДн | Подтверждение обработки ПДн | 30 дней (согласно пункту 1 статьи 20 152-ФЗ) | Подтверждение обработки ПДн |
| Отказ подтверждения обработки ПДн | 30 дней (согласно пункту 2 статьи 20 152-ФЗ) | Уведомление об отказе подтверждения обработки ПДн |
| 1.2. | Ознакомление с ПДн | Предоставление информации по ПДн | 30 дней (согласно пункту 1 статьи 20 152-ФЗ) | 1. Подтверждение обработки ПДн, а также правовые основания и цели такой обработки.  2. Способы обработки ПДн.  3. Сведения о лицах, которые имеют доступ к ПДн.  4. Перечень обрабатываемых ПДн и источник их получения.  5. Сроки обработки ПДн, в том числе сроки их хранения.  6. Информация об осуществленных или о предполагаемой трансграничной передаче.  7. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу. |
| Отказ предоставления информации по ПДн | 30 дней (согласно пункту 2 статьи 20 152-ФЗ) | Уведомление об отказе предоставления информации |
| 1.3. | Уточнение ПДн | Изменение ПДн | 7 рабочих дней со дня предоставления уточняющих сведений (согласно пункту 3 статьи 20 152-ФЗ) | Уведомление о внесенных изменениях |
| Отказ изменения ПДн | Уведомление об отказе изменения ПДн |
| 1.4. | Уничтожение ПДн | Уничтожение ПДн | 7 рабочих дней со дня предоставления сведений о незаконном получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ) | Уведомление об уничтожении |
| Отказ уничтожения ПДн | Уведомление об отказе уничтожения ПДн |
| 1.5. | Отзыв согласия на обработку ПДн | Прекращение обработки и уничтожение ПДн | 30 дней (согласно пункту 5 статьи 21 152-ФЗ) | Уведомление о прекращении обработки и уничтожении ПДн |
| Отказ прекращения обработки и уничтожения ПДн | Уведомление об отказе прекращения обработки и уничтожения ПДн |
| 1.6. | Недостоверность ПДн Субъекта | Блокировка ПДн | С момента обращения Субъекта ПДН о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ) | Уведомление о внесенных изменениях |
| Изменение ПДн | 7 рабочих дней со дня предоставления уточненных сведений (согласно пункту 2 статьи 21 152-ФЗ) |
| Снятие блокировки ПДн |
| Отказ изменения ПДн | Уведомление об отказе изменения ПДн |
| 1.7. | Неправомерность действий с ПДн Субъекта | Прекращение неправомерной обработки ПДн | 3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ) | Уведомление об устранении нарушений |
| Уничтожение ПДн в случае невозможности обеспечения правомерности обработки | 10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ) | Уведомление об уничтожении ПДн |
| 1.8. | Достижение целей обработки ПДн Субъекта | Прекращение обработки ПДн | 30 дней (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором с субъектом ПДн | Уведомление об уничтожении ПДн |
| Уничтожение ПДн |
| II. Запрос Уполномоченного органа по защите прав Субъекта ПДн | | | | |
| 2.1. | Информация для осуществления деятельности уполномоченного органа | Предоставление затребованной информации по ПДн | 30 дней (согласно пункту 4 статьи 20 152-ФЗ) | Предоставление затребованной информации по ПДн |
| 2.2. | Недостоверность ПДн Субъекта | Блокировка ПДн | С момента обращения Уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ) | Уведомление о внесенных изменениях |
| Изменение ПДн | 7 рабочих дней со дня предоставления уточненных сведений (согласно пункту 2 статьи 21 152-ФЗ) |
| Снятие блокировки ПДн |
| Отказ изменения ПДн | Уведомление об отказе изменения ПДн |
| 2.3. | Неправомерность действий с ПДн Субъекта | Прекращение неправомерной обработки ПДн | 3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ) | Уведомление об устранении нарушений |
| Уничтожение ПДн в случае невозможности обеспечения правомерности обработки | 10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ) | Уведомление об уничтожении ПДн |
| 2.4. | Достижение целей обработки ПДн Субъекта | Блокировка ПДн | 30 дней (согласно пункту 4 статьи 21 152-ФЗ), если иное не предусмотрено договором с субъектом ПДн | Уведомление об уничтожении ПДн |
| Уничтожение ПДн |

*Приложение № 11*

*к распоряжению*

*Главы Администрации*

*местного самоуправления*

*Моздокского района*

*№1014 от 23.08.2023 г.*

ЖУРНАЛ

учета хранилищ материальных носителей персональных данных Администрации местного

самоуправления Моздокского района Республики Северная Осетия-Алания

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ДДата | Наименование хранилища (сейф, металлический шкаф) | Инвентарный номер | Местонахождение  (подразделение,  номер комнаты) | Что находится (документы, изделия) | Ф.И.О.  Ответственного  за сейф (шкаф) | Кол-во комплектов ключей и их номера | Подпись  ответственного за  хранилище о выдаче  ключа и дата | Подпись, подтверж­дающая получение ключа, и дата |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета средств защиты информации, эксплуатационной и технической документации к ним в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

| №  п/п | Индекс и наименование средств защиты информации | Серийный (заводской) номер | Номер специального защитного знака | Наименование организации, установившей СЗИ | Место установки | Примечание |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

ЖУРНАЛ

учета мероприятий по контролю обеспечения защиты информации

Администрации местного самоуправления Моздокского района

Республики Северная Осетия-Алания

| №  п/п | Мероприятие | Дата | Исполнитель  (ФИО, подпись) | Результат |
| --- | --- | --- | --- | --- |
| 11 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

ЖУРНАЛ

регистрации обращений субъектов персональных данных, чьи персональные данные

обрабатываются в Администрации местного самоуправления Моздокского района

Республики Северная Осетия-Алания

| №  п/п | Дата поступления обращения | ФИО, адрес субъекта | Исполнитель | Исх. №,  дата ответа | Дата,  способ отправки | Примечание |
| --- | --- | --- | --- | --- | --- | --- |
| 11 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

ЖУРНАЛ

поэкземплярного учета средств криптографической защиты информации,

эксплуатационной и технической документации к ним, ключевых документов

Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

| № п.п. | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| От кого получены | Дата и номер сопроводительного | Ф.И.О. пользователя криптосредств | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |

ЖУРНАЛ

проведения инструктажей по информационной безопасности в Администрации

местного самоуправления Моздокского района Республики Северная Осетия-Алания

| № п/п | Инструктаж | | Инструктируемый | | Инструктирующий | |
| --- | --- | --- | --- | --- | --- | --- |
| Дата | Тема | ФИО | Подпись | ФИО | Подпись |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

ЖУРНАЛ

учета проведения ознакомления работников с законодательством и локальными актами по персональным данным в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

| № п/п | Фамилия, имя, отчество работника | Дата проведения ознакомления | Подпись работника | Подпись должностного лица, проводившего ознакомление | |
| --- | --- | --- | --- | --- | --- |
| ФИО | Подпись |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

ЖУРНАЛ

учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | Ф.И.О. ответственного за обеспечение безопасности персональных данных, подпись | Ф.И.О. администратора информационной системы, подпись | Примечание |
| --- | --- | --- | --- | --- | --- |
| 11 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

ЖУРНАЛ

учета съемных машинных носителей персональных данных в Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания

| № п/п | Тип носителя | Номер (серийный/инвентарный) | Расписка в получении | | | Подпись ответственного лица | Место хранения | Примечание | Дата и номер акта уничтожения |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ф.И.О. | дата | подпись |
| 11 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета проверок Администрации местного самоуправления Моздокского района Республики Северная Осетия-Алания, проводимых органами государственного контроля (надзора), органами муниципального контроля

| № п/п | Дата начала и окончания проверки | Общее время проведения проверки (в часах) | Наименование органа государственного, муниципального контроля | Дата и номер распоряжения (приказа) о проведении проверки | Цель, задачи и предмет проверки | Вид проверки (плановая, внеплановая) | Дата и номер акта, составленного по результатам проверки, дата вручения | Выявленные нарушения (содержание нарушения со ссылкой на положение нормативного акта) | Дата, номер и содержание предписания об устранении нарушений | Ф.И.О., должность лица проводившего проверку | Ф.И.О.должности экспертов, представителей экспертных организаций | Подпись должностного лица, проводившего проверку |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |