МИНИСТЕРСТВО ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ РЕСПУБЛИКИ ДАГЕСТАН

П Р И К А З

30 декабря 2015 г. г. Махачкала № 147

«Об обработке персональных данных в Министерстве по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий Республики Дагестан»

В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03. 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», п р и к а з ы в а ю :

1. Утвердить Правила обработки персональных данных в МЧС Дагестана (Приложение № 1).

2. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей в МЧС Дагестана (Приложение № 2).

3. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных в МЧС Дагестана требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (Приложение № 3).

4. Утвердить Правила работы с обезличенными данными в случае обезличивания персональных данных в МЧС Дагестана (Приложение № 4).

5. Утвердить Перечень должностей служащих МЧС Дагестана, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных (Приложение № 5).

6. Утвердить Перечень должностей служащих МЧС Дагестана, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным (Приложение № 6).

7. Утвердить Инструкцию пользователя информационных систем персональных данных МЧС Дагестана (Приложение № 7).

8. Утвердить перечень мест хранения материальных (бумажных и машинных) носителей персональных данных в МЧС Дагестана (Приложение № 8).

9. Утвердить форму журнала учета отчуждаемых машинных носителей персональных данных (Приложение № 9).

10. Утвердить перечень помещений, в которых размещены информационные системы персональных данных МЧС Дагестана (Приложение № 10).

11. Утвердить порядок доступа сотрудников МЧС Дагестана в помещения, в которых осуществляется обработка персональных данных и размещены информационные системы персональных данных (Приложение № 11).

12. Приказ МЧС Дагестана от 08.04.2015 г. № 35 «Об обработке персональных данных в Министерстве по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий Республики Дагестан» считать утратившим силу.

13. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Республики Дагестан в установленном законодательством порядке.

14. Разместить настоящий приказ на официальном сайте Министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий Республики Дагестан (www. mchs.e-dag.ru).

15. Настоящий приказ вступает в силу в установленном законодательством порядке.

16. Контроль за исполнением настоящего приказа возложить на заместителя министра Маллаева Д.Г.

Министр Н. Казимагамедов

Приложение № 1
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Правила обработки персональных данных в МЧС Дагестана

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в МЧС Дагестана (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07. 2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03. 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют цели обработки персональных данных, категории субъектов, персональные данные которых обрабатываются в МЧС Дагестана (далее – министерство, Оператор), содержание обрабатываемых персональных данных, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

2. Цели обработки персональных данных

2.1. Обработка персональных данных министерством осуществляется в следующих целях:

- ведение бухгалтерского учета;
- ведение кадрового учета;
- рассмотрение обращений граждан;
- проведение конкурса на замещение вакантных должностей государственной гражданской службы;
- антикоррупционная деятельность;
- осуществление и выполнение возложенных законодательством Российской Федерации и Республики Дагестан функций, полномочий и обязанностей.

2.2. Принципы, в соответствии с которыми осуществляется обработка персональных данных, приведены в Политике в отношении обработки персональных данных в МЧС Дагестана.

3. Категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения

3.1. В министерстве осуществляется обработка следующих категорий субъектов

персональных данных:

– государственные гражданские служащие;

– физические лица, с которыми заключен договор гражданско-правового характера;

– граждане, персональные данные которых необходимы для выполнения возложенных законодательством Российской Федерации и Республики Дагестан функций, полномочий и обязанностей;

– граждане, персональные данные которых необходимы для оказания муниципальных и государственных услуг;

– близкие родственники государственных гражданских служащих, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Республике Дагестан;

– граждане, персональные данные которых необходимы для рассмотрения обращений граждан;

– граждане, претендующие на замещение вакантной должности государственной гражданской службы.

3.2. Персональные данные обрабатываются в сроки, обусловленные заявленными целями их обработки.

3.3. Обработка персональных данных осуществляется с момента их получения министерством и прекращается:

– по достижении целей обработки персональных данных;

– в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных.

3.4. Сроки хранения персональных данных, содержащиеся на материальных носителях информации, устанавливаются в соответствии с номенклатурой дел министерства.

4. Содержание обрабатываемых персональных данных

4.1. В соответствии с целями обработки персональных данных, указанными в 2.1 настоящих Правил, министерством осуществляется обработка следующих персональных данных:

4.1.1. Государственные гражданские служащие:

– ФИО;

– сведения о смене ФИО;

– дата рождения;

– место рождения;

– гражданство;

– сведения об изменении гражданства;

– сведения о наличии гражданства другого государства;

– адрес регистрации;

- адрес проживания;
- контактные телефоны;
- контактные телефоны (или иной вид связи);
- данные документа, удостоверяющего личность;
- наименование органа, выдавшего документ, удостоверяющий личность;
- дата выдачи документа, удостоверяющего личность;
- данные заграничного паспорта;
- банковские реквизиты;
- ИНН;
- СНИЛС;
- реквизиты документа об образовании;
- сведения об образовании;
- направление подготовки или специальность по документу об образовании;
- квалификация по документу об образовании;
- сведения о послевузовском профессиональном образовании;
- должность;
- сведения о замещаемой должности;
- стаж работы;
- сведения о трудовой деятельности;
- классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы;
- сведения о детях;
- отношение к воинской обязанности и воинское звание;
- данные трудовой книжки;
- реквизиты трудовой книжки;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о государственных наградах;
- сведения о наградах (поощрениях);
- ученая степень;
- ученое звание;
- характеристика;
- сведения о пенсиях;
- номер счета;
- сведения о близких родственниках;
- сведения об изменении ФИО близкими родственниками;

– сведения о близких родственниках, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство;

– адрес электронной почты;

– сумма;

– размер оклада;

– сведения о пребывании за границей;

– сведения о доходах, налогах, страховых взносах;

– сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

– сведения о владении иностранными языками;

– сведения о стажировке;

– данные свидетельства о государственной регистрации права собственности;

– сведения о допуске к государственной тайне;

– фотография;

– сведения о судимости;

– сведения о наличии/отсутствии заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению.

4.1.2. Физические лица, с которыми заключен договор гражданско-правового характера:

– ФИО;

– дата рождения;

– данные документа, удостоверяющего личность;

– наименование органа, выдавшего документ, удостоверяющий личность;

– дата выдачи документа, удостоверяющего личность;

– ИНН;

– СНИЛС;

– номер счета;

– ФИО; данные документа, удостоверяющего личность; наименование органа, выдавшего документ, удостоверяющий личность; дата выдачи документа, удостоверяющего личность; ИНН; СНИЛС; номер счета; сумма; размер оклада; сведения о доходах, налогах, страховых взносах..

4.1.3. Граждане, персональные данные которых необходимы для выполнения возложенных законодательством Российской Федерации и Республики Дагестан функций, полномочий и обязанностей:

– ФИО;

– контактные телефоны;

– должность;

– адрес электронной почты.

4.1.4. Граждане, персональные данные которых необходимы для оказания муниципальных и государственных услуг:

– ФИО;
– дата рождения;
– место рождения;
– пол;
– гражданство;
– адрес регистрации;
– адрес проживания;
– контактные телефоны;
– данные документа, удостоверяющего личность;
– наименование органа, выдавшего документ, удостоверяющий личность;
– дата выдачи документа, удостоверяющего личность;
– ИНН;
– СНИЛС;
– адрес электронной почты.

4.1.5. Близкие родственники государственных гражданских служащих, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Республике Дагестан:

– ФИО;
– дата рождения;
– место рождения;
– степень родства;
– сведения о близких родственниках, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство;
– сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
– сведения о регистрации по месту жительства.

4.1.6. Граждане, персональные данные которых необходимы для рассмотрения обращений граждан:

– ФИО;
– адрес проживания;
– контактные телефоны;
– контактные телефоны (или иной вид связи);
– адрес электронной почты.

4.1.7. Граждане, претендующие на замещение вакантной должности государственной гражданской службы:

– ФИО;
– сведения о смене ФИО;
– дата рождения;

- место рождения;
- гражданство;
- сведения об изменении гражданства;
- сведения о наличии гражданства другого государства;
- адрес регистрации;
- адрес проживания;
- контактные телефоны (или иной вид связи);
- данные документа, удостоверяющего личность;
- наименование органа, выдавшего документ, удостоверяющий личность;
- дата выдачи документа, удостоверяющего личность;
- данные заграничного паспорта;
- ИНН;
- СНИЛС;
- реквизиты документа об образовании;
- сведения об образовании;
- направление подготовки или специальность по документу об образовании;
- квалификация по документу об образовании;
- сведения о послевузовском профессиональном образовании;
- сведения о трудовой деятельности;
- классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы;
- отношение к воинской обязанности и воинское звание;
- сведения о государственных наградах;
- ученая степень;
- ученое звание;
- сведения о близких родственниках;
- сведения о близких родственниках, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство;
- сведения о пребывании за границей;
- сведения о владении иностранными языками;
- сведения о допуске к государственной тайне;
- фотография.

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

5.1. В случае достижения цели обработки персональных данных Оператор обязан

прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим федеральными законами.

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

5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан 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.

5.4. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах5.1 – 5.3 настоящих Правил, Оператор осуществляет

блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.5. Уничтожение документов, содержащих персональные данные, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения персональных данных по утвержденной министерством форме.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

6.1. Министерство устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

– издание локальных актов по вопросам обработки и защиты персональных данных;

– назначение ответственного за организацию обработки персональных данных;

– определение лиц, уполномоченных на обработку персональных данных, министерства, несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима обработки персональных данных;

– ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику министерства в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников;

– получение согласий на обработку персональных данных у субъектов персональных данных (их законных представителей) за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике министерства в отношении обработки персональных данных, локальным актам министерства;

– опубликование на официальном сайте министерства документов, определяющих политику министерства в отношении обработки персональных данных, реализуемые требования к защите персональных данных;

– применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с требованиями Федерального закона «О персональных данных».

Приложение № 2
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Правила рассмотрения запросов субъектов персональных данных или их представителей в МЧС Дагестана

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в МЧС Дагестана (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07. 2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03. 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и определяют права субъектов персональных данных, обязанности МЧС Дагестана (далее – министерство, Оператор) при обращении субъекта персональных данных или его представителя, а также сроки и последовательность действий должностных лиц министерства при рассмотрении запросов субъектов персональных данных или их представителей (далее – Запрос).

1.2. Представитель субъекта персональных данных – лицо, действующее от имени субъекта персональных данных в силу полномочий, основанных на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления. При обращении представителя субъекта персональных данных в министерство представляется документ, подтверждающий полномочия законного представителя.

2. Права субъектов персональных данных

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

- подтверждение факта обработки персональных данных министерством;
- правовые основания и цели обработки персональных данных;
- цели и применяемые министерством способы обработки персональных данных;
- наименование и место нахождения министерства, сведения о лицах (за исключением работников министерства), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с министерством или 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 законодательством в сфере защиты

персональных данных;

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

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию о трансграничной передаче персональных данных;

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

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

2.2. Сведения, указанные в п.2.1 настоящих Правил, должны быть предоставлены субъекту персональных данных министерством 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.

2.3. Сведения, указанные в п.2.1 настоящих Правил, предоставляются субъекту персональных данных или его представителю министерством при обращении либо при получении запроса субъекта персональных данных или его представителя. 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 министерством (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных министерством, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2.4. В случае, если сведения, указанные в п.2.1 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в министерство или направить повторный запрос в целях получения сведений, указанных в п.2.1 настоящих Правил, 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.

2.5. Субъект персональных данных вправе обратиться повторно в министерство или направить повторный запрос в целях получения сведений, указанных в п.2.1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п.2.4 настоящих Правил, 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 со сведениями, указанными в п.2.3 настоящих Правил, должен содержать обоснование направления повторного запроса.

2.6. Министерство вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 2.4 и п. 2.5 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на министерстве.

2.7. Субъект персональных данных вправе требовать от министерства 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.

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

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

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

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

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

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

3. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя

3.1. Оператор обязан сообщить в порядке, предусмотренном настоящими

Правилами, 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.

3.2. 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 Оператор обязан дать в письменной форме мотивированный ответ, с указанием причин отказа со ссылкой на положение ч.8 ст.14 Федерального закона «О персональных данных» 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.

3.3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. 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, Оператор обязан внести в них необходимые изменения. 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, Оператор обязан уничтожить такие персональные данные. Оператор обязан 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.

4. Порядок рассмотрения запросов субъектов персональных данных или их представителей

4.1. В день поступления запроса субъекта персональных данных или его представителя в министерство указанный запрос необходимо зарегистрировать в соответствии с правилами документооборота, установленными министерством, а также внести соответствующую запись в Журнал учета обращений субъектов персональных данных. Форма Журнала учета обращений субъектов персональных данных утверждена нормативным актом министерства.

4.2. Ответственный за организацию обработки персональных данных министерства осуществляет непосредственный контроль за соблюдением установленного

законодательством Российской Федерации и настоящими Правилами порядка рассмотрения запросов субъектов персональных данных или их представителей. На контроль берутся все запросы.

4.3. Структурное подразделение, ответственное за исполнение указанного запроса, обеспечивает рассмотрение запроса и подготовку необходимой информации в установленный действующим законодательством срок.

4.4. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

4.5. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудником министерства действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются руководителю министерства.

4.6. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

4.7. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение № 3
к приказу МЧС Дагестана
от _____._____. 2015г. № ____

Правила осуществления внутреннего контроля соответствия обработки персональных данных в МЧС Дагестана требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в МЧС Дагестана требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07. 2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МЧС Дагестана (далее – министерство) проводятся периодические проверки условий обработки персональных данных.

2.2. Проверка соответствия обработки персональных данных требованиям к защите персональных данных проводится ответственным за организацию обработки персональных данных.

2.3. Плановые проверки условий обработки персональных данных проводятся на основании утвержденного руководителем министерства ежегодного плана внутренних проверок режима защиты персональных данных (плановые проверки), представленного в приложении к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МЧС Дагестана.

2.4. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки персональных данных. Проведение внеплановой проверки

организуется в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

2.5. В проведении проверки условий обработки персональных данных не могут участвовать сотрудники министерства, прямо или косвенно заинтересованные в ее результатах.

2.6. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников министерства, участвующих в процессе обработки персональных данных.

2.7. При проведении проверки условий обработки персональных данных должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;

– порядок и условия соблюдения парольной защиты;

– порядок и условия соблюдения антивирусной защиты;

– порядок и условия обеспечения резервного копирования;

– эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в информационные системы персональных данных;

– условия соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена;

– порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационной системы персональных данных;

– порядок и условия применения средств защиты информации;

– состояние учета носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Проверка условий обработки персональных данных должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

2.9. По результатам проведенной проверки условий обработки персональных данных ответственный за организацию обработки персональных данных предоставляет руководителю министерства письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.

Приложение № 4
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Правила работы с обезличенными данными в случае обезличивания персональных данных в МЧС Дагестана

1. Общие положения

1.1. Правила работы с обезличенными данными в случае обезличивания персональных данных в МЧС Дагестана (далее – Правила) разработаны в соответствии с требованиями Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09. 2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и определяют условия обезличивания персональных данных, методы обезличивания персональных данных и порядок работы с обезличенными данными.

2. Условия обезличивания персональных данных

2.1. В соответствии с Федеральным законом «О персональных данных» обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.2. Обезличивание персональных данных может быть проведено в статистических целях, в целях предупреждения ущерба от разглашения персональных данных, по достижении целей или в случае утраты необходимости в достижении этих целей, а также в иных целях, предусмотренных законодательством Российской Федерации.

2.3. Обезличивание персональных данных должно обеспечивать следующие свойства информации:

– полноту (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);

– структурированность (сохранение структурных связей между обезличенными персональными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);

– релевантность (возможность обработки запросов по обработке персональных

данных и получения ответов в одинаковой семантической форме);

– семантическую целостность (сохранение семантики (сути и смысла) персональных данных при их обезличивании);

– применимость (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных без предварительного деобезличивания всего объема записей о субъектах);

– анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

2.4. Методы обезличивания персональных данных должны обладать следующими характеристиками:

– обратимостью (возможностью преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);

– вариативностью (возможностью внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

– изменяемостью (возможностью внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

– стойкостью (стойкостью метода к атакам на идентификацию субъекта персональных данных);

– возможностью косвенного деобезличивания (возможностью проведения деобезличивания с использованием информации других операторов);

– совместимостью (возможностью интеграции персональных данных, обезличенных различными методами);

– параметрическим объемом (возможностью определения объема дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

– возможностью оценки качества данных (возможностью проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

2.5. Методы обезличивания персональных данных должны обладать следующими свойствами:

– обратимостью (возможность проведения деобезличивания);

– возможностью обеспечения заданного уровня анонимности;

– увеличением стойкости при увеличении объема обезличиваемых персональных данных.

2.6. Получаемые обезличенные данные должны обладать следующими свойствами:

– сохранением полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

– сохранением структурированности обезличиваемых персональных данных;

– сохранением семантической целостности обезличиваемых персональных данных;

– анонимностью отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

2.7. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

2.8. В МЧС Дагестана (далее – министерство) могут быть использованы следующие методы обезличивания:

– метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

– метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

– метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

– метод перемешивания (перестановка отдельных записей, а так же групп записей в массиве персональных данных).

2.9. Описание методов обезличивания, обеспечиваемых ими свойств обезличенных данных, оценка свойств методов, требования к реализации методов приведены в приложении к настоящим Правилам.

2.10. Предложения о методах обезличивания вносит ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных министерства. Решение о методах обезличивания персональных данных принимает руководитель министерства.

2.11. Ответственность за обезличивание персональных данных несут лица, замещающие должности, вошедшие в Перечень должностей служащих МЧС Дагестана, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных.

3. Порядок работы с обезличенными данными

3.1. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

3.2. Обезличенные персональные данные могут обрабатываться как с использованием, так и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных сотрудники министерства руководствуются настоящими Правилами.

Приложение
к Правилам работы с обезличенными данными в
случае обезличивания персональных данных в
МЧС Дагестана

Описание методов обезличивания

1. Метод введения идентификаторов

1.1. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

1.2. Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- семантическая целостность;
- применимость.

1.3. Оценка свойств метода:

- обратимость (метод позволяет провести процедуру деобезличивания);
- вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);
- изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);
- стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
- возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
- совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);
- параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах персональных данных, подлежащих обезличиванию);
- возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

1.4. Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

2. Метод изменения состава или семантики

2.1. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

2.2. Метод обеспечивает следующие свойства обезличенных данных:

- структурированность;
- релевантность;
- применимость;
- анонимность.

2.3. Оценка свойств метода:

- обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);
- вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);
- изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
- стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
- возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
- совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);
- параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);
- возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).

2.4. Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта. При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

3. Метод декомпозиции

3.1. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

3.2. Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;

– релевантность;
– семантическая целостность;
– применимость.

3.3. Оценка свойств метода:

– обратимость (метод позволяет провести процедуру деобезличивания);
– вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);
– изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
– стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);
– возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
– совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);
– параметрический объем (определяется числом подмножеств и числом субъектов персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);
– возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

3.4. Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

4. Метод перемешивания

4.1. Метод перемешивания реализуется путем перемешивания отдельных записей, а так же групп записей между собой.

4.2. Метод обеспечивает следующие свойства обезличенных данных:

– полнота;
– структурированность;
– релевантность;
– семантическая целостность;
– применимость;
– анонимность.

4.3. Оценка свойств метода:

– обратимость (метод позволяет провести процедуру деобезличивания);
– вариативность (метод позволяет изменять параметры перемешивания без

проведения процедуры деобезличивания);

– изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

– стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);

– возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);

– совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);

– параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);

– возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

4.4. Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

4.5. Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

Приложение № 5
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Перечень должностей служащих МЧС Дагестана, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных

№ п/п	Структурное подразделение	Должность
1.	Руководство министерства	Заместители министра
2.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Начальник отдела
3.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Ведущие специалисты 2 разряда
4.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Старшие специалисты 1 разряда
5.	Отдел финансового, материально-технического обеспечения и контрактной службы	Начальник отдела
6.	Отдел финансового, материально-технического обеспечения и контрактной службы	Ведущие специалисты 2 разряда
7.	Отдел финансового, материально-технического обеспечения и контрактной службы	Старшие специалисты 1 разряда

Приложение № 6
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Перечень должностей служащих МЧС Дагестана, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным

№ п/п	Структурное подразделение	Должность
1.	Руководство министерства	Заместители министра
2.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Начальник отдела
3.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Ведущие специалисты 2 разряда
4.	Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной тайны	Старшие специалисты 1 разряда
5.	Отдел финансового, материально-технического обеспечения и контрактной службы	Начальник отдела
6.	Отдел финансового, материально-технического обеспечения и контрактной службы	Ведущие специалисты 2 разряда
7.	Отдел финансового, материально-технического обеспечения и контрактной службы	Старшие специалисты 1 разряда

Приложение № 7
к приказу МЧС Дагестана
от _____._____. 2015г. № _____

Инструкция пользователя
информационных систем персональных данных
МЧС Дагестана

1. Общие положения

1.1. Пользователем информационных систем персональных данных (далее – Пользователь) является уполномоченный сотрудник МЧС Дагестана (далее – министерство).

1.2. Пользователь должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки персональных данных.

1.3. В своей деятельности, связанной с обработкой персональных данных, Пользователь руководствуется Политикой в отношении обработки персональных данных в МЧС Дагестана и настоящей Инструкцией.

1.4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.

2. Обязанности и права пользователя информационных систем персональных данных

2.1. Пользователь обязан:

– соблюдать требования Политики в отношении обработки персональных данных в МЧС Дагестана и иных нормативных актов министерства, устанавливающих порядок работы с персональными данными;

– выполнять в информационных системах персональных данных (далее – ИСПДн) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

– использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера (автономной ПЭВМ);

– пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

– обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

– немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение безопасности персональных данных в ИСПДн (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

– перед началом обработки в ИСПДн файлов, хранящихся на съемных носителях информации, Пользователь должен осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;

– располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

2.2. Пользователям ИСПДн запрещается:

– записывать и хранить информацию, относящуюся к конфиденциальной информации или персональным данным, на неучтенных материальных носителях информации;

– оставлять во время работы материальные носители информации без присмотра, не санкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;

– отключать средства антивирусной защиты;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;

– сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПДн;

– работать в ИСПДн при обнаружении каких-либо неисправностей;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– вводить в ИСПДн персональные данные под диктовку или с микрофона;

– привлекать посторонних лиц для производства ремонта технических средств ИСПДн без согласования с Ответственным.

2.3. Пользователь имеет право знакомиться с внутренними документами министерства, регламентирующими его обязанности по занимаемой должности.

3. Организация парольной защиты при работе на объектах информатизации

3.1. Пароли доступа к ИСПДн устанавливаются Ответственным или Пользователем.

3.2. При формировании пароля необходимо руководствоваться следующими требованиями:

– длина пароля должна быть не менее 8-и буквенно-цифровых символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

– запрещается использовать ранее использованные пароли.

3.3. При организации парольной защиты запрещается:

– записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

– хранить пароли в записанном виде на отдельных листах бумаги;

– сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.

4. Порядок применения парольной защиты

4.1. Плановую смену паролей на доступ в ИСПДн рекомендуется проводить один раз в месяц.

4.2. Пользователь обязан незамедлительно сообщить Ответственному факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

4.3. Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

– компрометации (подозрении на компрометацию) пароля;

– в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы данного с ИСПДн);

– по инициативе Ответственного.

5. Технология обработки персональных данных

5.1. При первичном допуске к работе с ИСПДн Пользователь:

– проходит инструктаж по использованию ИСПДн;

– знакомится с требованиями нормативно-правовых, руководящих и организационно-распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных;

– получает у Ответственного идентификатор и личный пароль для входа в ИСПДн.

5.2. Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

5.3. Авторизацию в ИСПДн (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

5.4. В процессе работы на АРМ ИСПДн Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИСПДн.

5.5. Копирование персональных данных на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

5.6. При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих персональные данные, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

5.7. Печать документов, содержащих персональные данные, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно с применением уничтожителей бумаги. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих персональные данные, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.

5.8. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПДн, Пользователь обязан выключить компьютер, либо заблокировать его, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих министерства, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

5.9. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

Приложение № 8
к приказу МЧС Дагестана
от _____._____. 2015г. № _____

Перечень мест хранения материальных (бумажных и машинных) носителей персональных данных в МЧС Дагестана

№ п/ п	Категория субъекта персональных данных	Адрес места расположения, наименование структурного подразделения, наименование помещения
Цель обработки персональных данных: ведение кадрового учета		
1.	Государственные гражданские служащие	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 414;415 Отдел финансового, материально-технического обеспечения и контрактной службы - кабинет № 402;404
2.	Близкие родственники государственных гражданских служащих, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Российской Федерации	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 414;415 Отдел финансового, материально-технического обеспечения и контрактной службы - кабинет № 402;404
3.	Физические лица, с которыми заключен договор гражданско-правового характера	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 414;415 Отдел финансового, материально-технического обеспечения и контрактной службы - кабинет № 402;404
Цель обработки персональных данных: рассмотрение обращений граждан		
4.	Граждане, персональные данные которых необходимы для рассмотрения обращений граждан	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 413;414;415
Цель обработки персональных данных: проведение конкурса на замещение вакантных должностей государственной гражданской службы		
5.	Граждане, претендующие на замещение вакантной должности государственной гражданской	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения,

№ п/ п	Категория субъекта персональных данных	Адрес места расположения, наименование структурного подразделения, наименование помещения
	службы	делопроизводства и защиты государственной защиты - кабинет № 414;415
Цель обработки персональных данных: антикоррупционная деятельность		
6.	Государственные гражданские служащие	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 414;415
7.	Близкие родственники государственных гражданских служащих, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Российской Федерации	***367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»:*** Отдел кадрового, правового обеспечения, делопроизводства и защиты государственной защиты - кабинет № 414;415

Приложение № 9
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Журнал учета отчуждаемых машинных носителей персональных данных

Учетный/ регистрационный (заводской) номер	Дата постановки на учет	Вид машинного носителя	Место хранения (размещения)*	Лицо, ответственное за использование и хранение					Отметка об уничтожении	
				Ф.И.О., должность	Дата получения	Подпись	Дата возврата	Подпись	Дата и № акта	Подпись ответственного лица
1	2	3	4	5	6	7	8	9	10	11

* в случае если на отчуждаемом машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов)

Приложение № 10
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Перечень помещений, в которых размещены информационные системы персональных данных МЧС Дагестана

Перечень помещений, в которых размещена информационная система персональных данных «1С-Бухгалтерия» МЧС Дагестана

№ п/п	Адрес места расположения	Наименование структурного подразделения, наименование помещения
1.	367015, Республика Дагестан, г. Махачкала, ул. М. Ярагского, д. 124 «а»	Отдел финансового, материально-технического обеспечения и контрактной службы - кабинет № 402;404

Приложение № 11
к приказу МЧС Дагестана
от ____._____. 2015г. № ____

Порядок доступа сотрудников МЧС Дагестана в помещения, в которых осуществляется обработка персональных данных и размещены информационные системы персональных данных

Настоящий Порядок регламентирует условия и порядок осуществления доступа сотрудников МЧС Дагестана (далее – министерство) в помещения, в которых осуществляется обработка персональных данных и размещены информационные системы персональных данных (далее – Помещения) в целях организации режима обеспечения безопасности информации, содержащей персональные данные, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа.

Настоящий Порядок разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 11.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки персональных данных, средств защиты информации и носителей персональных данных, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

В помещения, где размещены информационные системы, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, содержащей персональные данные, допускаются только сотрудники министерства, уполномоченные на обработку персональных данных. Перечень сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в информационных системах персональных данных (далее – Сотрудники), утверждается нормативным актом министерства. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

Нахождение в Помещениях посторонних лиц допускается только в сопровождении Сотрудников министерства.

Уборка и техническое обслуживание Помещений допускаются только в присутствии Сотрудников министерства.

О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю структурного подразделения министерства.

Двери Помещений должны быть оборудованы механическими замками.

Перед началом рабочего (служебного) времени Сотрудники министерства берут ключи от Помещений с внесением записи в журнал.

В течение рабочего (служебного) времени ключи от Помещений хранятся у Сотрудников министерства.

По окончании рабочего (служебного) времени Сотрудники министерства закрывают Помещения и сдают ключи с внесением записи в журнал.

Внутренний контроль за соблюдением порядка доступа в Помещения проводится лицом, ответственным за организацию обработки персональных данных.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О.	Должность	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				