Къэбэрдей-Балъкъэр Республикэм
лэжьыгъэмкIэ, цIыхухэр лэжьапIэкIэ
къыззэгъэпэщынымкIэ, социальнэу
хъумэнымкIэ и министерствэ

Къабарты-Малкъар Республиканы
урунуу, иш бла жалчытыу
эм социальный жаны бла
къоруулау министерствосу

МИНИСТЕРСТВО ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ

(МИНТРУДСОЦЗАЩИТЫ КБР)

ПРИКАЗ № 229-п

«24» июля 2015 г. г. Нальчик

Об утверждении Политики в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики в отношении обработки и защиты персональных данных

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

п р и к а з ы в а ю:

1. Утвердить прилагаемую Политику Министерства труда, занятости и социальной защиты Кабардино-Балкарской Республики в отношении обработки и защиты персональных данных.
2. Отделу автоматизации и информационных технологий информационно-аналитического департамента (Дажигова В.А.) обеспечить опубликование настоящего приказа на официальном Интернет-сайте министерства.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр А. Тюбеев

Утверждена
Приказом Министерства
труда, занятости и социальной защиты
Кабардино-Балкарской Республики
№____ от «__» _____ 2015 года

ПОЛИТИКА
В МИНИСТЕРСТВЕ ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Политика принята в целях сохранения личной тайны и защиты персональных данных (далее - ПДн), обрабатываемых в Министерстве труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - Министерство).

1.2. Политика определяет права и обязанности руководителей и сотрудников Министерства, порядок использования указанных данных в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения ПДн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Министерством как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Министр труда, занятости и социальной защиты Кабардино-Балкарской Республики (далее - Министр) определяет лиц из числа сотрудников Министерства, уполномоченных на обработку ПДн, обеспечивающих обработку ПДн в соответствии с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих ПДн.

1.5. Если в отношениях с Министерством участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Министерство становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Министерства распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Министерством.

2. Основные термины и определения

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. Оператор - государственный орган (Министерство), самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.3. 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.

2.4. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

2.6. 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.

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

2.8. Информационная система - информационная система, содержащая персональные данные государственных гражданских служащих Министерства.

3. Основания обработки персональных данных в Министерстве

3.1. Обработка ПДн в Министерстве осуществляется в связи с выполнением законодательно возложенных на Министерство полномочий и функций, определяемых Положением о Министерстве.

3.2. Кроме того, в Министерстве осуществляется обработка ПДн, связанных с поступлением на государственную гражданскую службу Кабардино-Балкарской Республики и ее прохождением, реализацией трудовых отношений, формированием кадрового резерва на государственную гражданскую службу Кабардино-Балкарской Республики в Министерстве.

4. Документы, которыми руководствуется Министерство при работе с персональными данными

4.1. Министерство при работе с ПДн руководствуется следующими документами:

- Конституция Российской Федерации от 12.12.1993;
- Федеральный закон №152-ФЗ от 27.07.2006 «О персональных данных»;
- Федеральный закон №160-ФЗ от 19.12.2005 «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи»;
- Трудовой кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях;
- Указ Президента Российской Федерации №188 от 06.03.1997 «Об утверждении Перечня сведений конфиденциального характера»;
- Указ Президента Российской Федерации №351 от 17.03.2008 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- распоряжение Президента Российской Федерации №366-рп от 10.07.2001 «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;
- Постановление Правительства Российской Федерации №1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации №211 от 21.03.2012 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами»;
- Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21.02.2008 №149/6/6-622;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 15.02.2008;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных утверждена ФСТЭК России 14.02.2008, а не 12.02.2008.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 12.02.2008.

5. Принципы обработки персональных данных

5.1. Обработка ПДн должна осуществляться на законной и справедливой основе.

5.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

5.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

5.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

5.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

5.6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Министерство принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

5.7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению или обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не

предусмотрено федеральным законом.

6. Круг субъектов, персональные данные которых подлежат обработке

6.1. Субъектами ПДн являются:

- физические лица - получатели государственных услуг, предоставляемых Министерством;
- лица, поступающие на государственную гражданскую службу Кабардино-Балкарской Республики и ее проходящие в Министерстве.

7. Источники получения персональных данных

7.1. Источниками ПДн являются субъекты ПДн, а также их законные представители.

7.2. ПДн могут быть получены Министерством в электронном виде или в бумажном виде. При передаче своих ПДн в электронном виде субъект ПДн дает свое согласие на их обработку, соглашаясь с правилами пользования информационным ресурсом Министерства.

8. Состав, порядок и цели обработки персональных данных

8.1. Состав, порядок и цели обработки ПДн в Министерстве в отношении:

- физических лиц - получателей государственных услуг, предоставляемых Министерством, определены в Административных регламентах по оказанию государственных услуг Министерством;
- лиц, поступающих на государственную гражданскую службу Кабардино-Балкарской Республики и ее проходящих в Министерстве, установлены положением об обработке и защите персональных данных в Министерстве, утверждаемым приказом Министерства.

8.2. Запрещено обрабатывать дополнительные ПДн.

9. Способы обработки персональных данных

9.1. Обработка ПДн в Министерстве осуществляется как с применением информационных технологий и технических средств в информационных системах (далее - ИС), так и без средств автоматизации. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, программные средства (операционные системы, системы управления базами данных и прочее), средства защиты информации, применяемые в информационных системах.

10. Носители персональных данных

10.1. Носителями ПДн являются:

- электронные носители - магнитные и оптические (CD и DVD) накопители, съемные жесткие диски и флеш-накопители, применяемые для получения информации;
- бумажные носители информации о ПДн.

11. Порядок организации делопроизводства документов, содержащих персональные данные

11.1 Документы, содержащие ПДн, относятся к защищаемой информации и требуют организации отдельного делопроизводства и хранения.

11.2. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители).

11.3. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы.

11.4. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

11.5. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

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

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

11.6. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11.7. Уничтожение ПДн на материальном носителе производится комиссией, созданной приказом Министерства, состоящей из сотрудников Министерства. При этом заполняется акт об уничтожении материальных носителей, содержащих ПДн, приведенный в приложении 1 к настоящей Политике.

11.8. Уточнение ПДн 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 ПДн.

12. Требования к типовым формам документов

12.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

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

б) типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, указанных в типовой форме, имел возможность ознакомиться со своими ПДн, содержащимися в форме, не нарушая прав и законных интересов иных субъектов ПДн;

г) типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо несовместимы.

13. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13.1. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

13.2. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

13.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

14. Требования к сотрудникам Министерства

14.1. Приказом Министерства назначается сотрудник Министерства, ответственный за обеспечение безопасности ПДн, при их обработке в ИС. В должностном регламенте ответственного за обеспечение безопасности ПДн должна быть отражена обязанность по обеспечению конфиденциальности ПДн и их безопасности при их обработке в ИС.

14.2. Для осуществления мероприятий по обработке ПДн в ИС назначается администратор безопасности, ответственный за обеспечение безопасности ПДн в процессе их обработки и передачи по каналам связи. Функции администратора безопасности для осуществления мероприятий по обработке ПДн в ИС могут выполняться как сотрудником Министерства, назначенным приказом Министерства, так и с привлечением сторонней организации по государственному контракту на условиях аутсорсинга.

14.3. Приказом Министерства утверждается перечень сотрудников Министерства, которым необходим доступ к ПДн, обрабатываемых в ИС, для выполнения своих должностных обязанностей.

14.4. При работе с ПДн в ИС лица, допущенные к обработке этих данных в процессе выполнения служебных обязанностей, должны обеспечивать:

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

б) своевременное обнаружение фактов несанкционированного доступа к ПДн;

в) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование и целостность данных;

г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности ПДн.

14.5. Требования к должностным лицам, работающим с ПДн в Министерстве, включаются в их должностные регламенты.

15. Порядок взаимодействия с субъектами персональных данных

15.1. Субъект ПДн имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора ПДн, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими ПДн. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

15.2. Сведения о наличии ПДн должны предоставляться субъекту ПДн оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

15.3. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при обращении либо при получении запроса субъекта ПДн или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

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

1) подтверждение факта обработки ПДн оператором;

2) правовые основания и цели обработки ПДн;

3) цели и применяемые оператором способы обработки ПДн;

4) наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

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

6) сроки обработки ПДн, в том числе сроки их хранения;

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

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

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

10) иные сведения, предусмотренные Федеральным законом N 152-ФЗ от 27.07.2006 "О персональных данных".

15.5. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если:

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

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру

пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

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

4) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн 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.

15.6. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

15.7. Оператор обязан разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

15.8. Оператор обязан разъяснить цели обработки ПДн субъекту ПДн. Оператор обязан рассмотреть возражение против автоматизированной обработки в течение тридцати дней со дня его получения и уведомить субъекта ПДн о результатах рассмотрения такого возражения.

15.9. Если субъект ПДн считает, что оператор осуществляет обработку его ПДн с нарушением требований Федерального закона N 152-ФЗ от 27.07.2006 "О персональных данных" или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

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

16. Реализация Политики

16.1. Министерство принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

16.2. Ответственность за организацию обработки ПДн в Министерстве несет должностное лицо Министерства, назначаемое приказом Министерства. Ответственный за организацию обработки ПДн в Министерстве, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Министерстве требований нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

2) доводить до сведения должностных лиц Министерства положения нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

16.3. При обработке ПДн без использования средств автоматизации Министерство в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПДн от информации, не содержащей ПДн;

2) раздельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые Министерством, или в иных аналогичных целях;

5) сохранность материальных носителей ПДн;

6) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПДн.

16.4. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн, обработки ПДн с использованием средств автоматизации в Министерстве создаются ИС.

16.5. ИС проходят классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн. Для ИС формируется модель угроз безопасности ПДн и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу ИС.

16.6. Пересмотр моделей угроз для ИС осуществляется:

а) в плановом порядке для существующих ИС - при изменении условий использования ИС;

б) в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИС - в течение трех месяцев с даты фиксации изменений;

в) в случае создания новой ИС (выделения части из существующей ИС) - в течение двух месяцев с даты создания (выделения) ИС.

16.7. Обработка ПДн в Министерстве с использованием средств автоматизации ведется только в ИС. В Министерстве запрещается обработка ПДн с целями, не соответствующими целям создания ИС, эксплуатация ИС в составе, отличном от указанного при создании ИС.

16.8. Ввод в эксплуатацию ИС оформляется актом ввода в эксплуатацию и сопровождается аттестацией ИС или декларированием соответствия ИС требованиям по безопасности ПДн в соответствии с нормативными правовыми актами в области обеспечения безопасности ПДн.

16.9. В целях обеспечения управления информационной безопасностью ПДн в Министерстве создается система защиты ПДн (далее - СЗПДн).

16.10. Объектами защиты СЗПДн являются информация, обрабатываемая Министерством и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

16.11 СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку внутренних регулятивных документов Министерства по вопросам обработки и защиты ПДн, контроль за исполнением в Министерстве требований

нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств должностных лиц о неразглашении ПДн;

3) доведение до сведения должностных лиц информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Министерства и должностных регламентах сотрудников Министерства требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Министерства по обеспечению информационной безопасности ИС;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление должностных лиц Министерства с положениями нормативных правовых актов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн и (или) организация обучения их правилам обработки и защиты ПДн;

8) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

а) физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Министерства, так и при взаимодействии с контрагентами Министерства, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

10) установление правил доступа на объекты, в помещения, в ИС, применение в этих целях систем охраны и управления доступом;

11) формирование участков (выделение в отдельные VLAN (виртуальные локальные компьютерные сети) технических средств) администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и ИС в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Министерстве (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Министерства в области обработки и защиты ПДн;

14) установление полномочий пользователей и форм представления информации пользователям ИС;

15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

16) организацию необходимых мероприятий с должностными лицами, а также собеседование с лицами, претендующими на работу в Министерстве, изучение их биографии и проверку предоставляемых сведений; обучение должностных лиц требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

а) при стратегическом планировании архитектуры ИС;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

19) применение следующих компонентов программно-технических мер защиты:

а) защищенных средств (систем) обработки информации, содержащей ПДн;

б) системы криптографической защиты информации при ее передаче по каналам связи;

в) межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

г) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

16.12. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИС разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях. Должностные лица проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

16.13. По окончании сроков обработки ПДн в ИС приказом Министерства создается комиссия из сотрудников Министерства для уничтожения ПДн. Данные ПДн уничтожаются и составляется акт об уничтожении, приведенный в приложении 2 к настоящей Политике.

17. Правила допуска, хранения и пересылки персональных данных

17.1. Допуск лиц к обработке ПДн в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

17.2. Пересылка ПДн без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

18. Ответственность за нарушение норм, регулирующих обработку персональных данных

18.1. Сотрудники Министерства, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

18.2. Неправомерный отказ исключить или исправить ПДн субъекта, а также любое иное нарушение прав субъекта на защиту ПДн влечет возникновение у субъекта права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

Приложение №1

Утверждены
Приказом Министерства
труда, занятости и социальной защиты
Кабардино-Балкарской Республики
№____ от «__» _____ 2015 года

АКТ
УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, НАХОДЯЩИХСЯ НА МАТЕРИАЛЬНЫХ НОСИТЕЛЯХ МИНИСТЕРСТВА ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОЙ ЗАЩИТЫ КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ

_____ «_____» _____ 20__ г.
Место уничтожения Дата уничтожения

Комиссия в составе:

Председатель комиссии:
_____ _____
Должность ФИО

Члены комиссии:
_____ _____
Должность ФИО
_____ _____
Должность ФИО
_____ _____
Должность ФИО

составили настоящий акт о том, что «____» _____ 20___ г. произведено уничтожение персональных данных, находящихся на бумажном носителе. Уничтожены персональные данные в соответствии с таблицей.

№	Информация (наименование документа)	Учетный номер документа	Количество	Срок хранения

Подписи членов комиссии:

Председатель комиссии:
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата

Члены комиссии:
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата

Приложение №1

Утверждены
Приказом Министерства
труда, занятости и социальной защиты
Кабардино-Балкарской Республики
№____ от «__» _____ 2015 года

АКТ
УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, НАХОДЯЩИХСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

_____ «_____» _____ 20__ г.
Место уничтожения Дата уничтожения

Комиссия в составе:

Председатель комиссии:
_____ _____
Должность ФИО

Члены комиссии:
_____ _____
Должность ФИО
_____ _____
Должность ФИО
_____ _____
Должность ФИО

составили настоящий акт о том, что «____» _____ 20___ г. произведено уничтожение персональных данных, находящихся на: _____
_____
(наименование АРМ по утвержденной конфигурации, ФИО ответственного пользователя, заводской номер системного блока ПЭВМ, носителя информации, способ уничтожения)
Уничтожены персональные данные в соответствии с таблицей.

№	Информация (наименование документа)	Учетный номер	Вид носителя	Количество	Срок хранения

Подписи членов комиссии:

Председатель комиссии:
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата

Члены комиссии:
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата
_____ _____ «__» _____ 201__ г.
Подпись ФИО Дата