МИНИСТЕРСТВО ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ И СПОРТУ РЕСПУБЛИКИ ДАГЕСТАН

ПРИКАЗ

"01" 04 2013 г. № 77

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ПО ФИЗИЧЕКОЙ КУЛЬТУРЕ И СПОРТУ РЕСПУБЛИКИ ДАГЕСТАН

В соответствии с требованиями Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30 мая 2005 года N 609, Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года N 781, и Закона Республики Дагестан от 12 октября 2005 года N 32 "О государственной гражданской службе Республики Дагестан" приказываю:

1. Утвердить Положение об обработке персональных данных в Министерстве по физической культуре и спорту Республики Дагестан (прилагается).

2. Руководителям структурных подразделений Министерства ознакомить государственных гражданских служащих, замещающих должности государственной гражданской службы Республики Дагестан в Министерстве (далее - государственные гражданские служащие), и работников Министерства с настоящим приказом.

3. Государственным гражданским служащим при обработке персональных данных руководствоваться требованиями утвержденного настоящим приказом Положения.

4.Ответственность за организацию обработки персональных данных в Министерстве возложить на заместителя министра по физической культуре и спорту Республики Дагестан Магомедова Г.М.

5. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. министра **З. Салаутдинов**

Приложение к приказу
Министерства по физической культуре
и спорту Республики Дагестан

от «01» 04 2013 г № 77

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ И СПОРТУ РЕСПУБЛИКИ ДАГЕСТАН

1. Настоящим Положением определяется порядок обработки, формирования и хранения персональных данных государственных гражданских служащих, замещающих должности государственной гражданской службы Республики Дагестан (далее - гражданские служащие) в Министерстве по физической культуре и спорту Республики Дагестан (далее - Министерство), работников Министерства, руководителей подведомственных учреждений находящихся в ведении Министерства, кандидатов на службу (работу), лиц, уволенных со службы (работы), электронных банков данных содержащих персональные данные спортсменов Республики Дагестан проходящих спортивную подготовку, обрабатываемых на основании полномочий Министерства, в целях защиты прав граждан на неприкосновенность частной жизни, личную и семейную тайну, а также установления ответственности должностных лиц, имеющих доступ к персональным данным, за нарушение требований норм, регулирующих обработку и защиту персональных данных.

2. Настоящее Положение разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", Трудовым кодексом Российской Федерации, Указом Президента Российской Федерации от 30 мая 2005 года N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела", постановлением Правительства Российской Федерации от 17 ноября 2007 года N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановлением Правительства Российской Федерации от 21.03.2012 N 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", Законом

Республики Дагестан от 12 октября 2005 года N 32 "О государственной гражданской службе Республики Дагестан" и другими нормативными правовыми актами.

3. В настоящем Положении используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных),, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия

субъекта персональных данных или наличия иного законного основания;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

4. Представитель нанимателя в лице министра по физической культуре и спорту Республики Дагестан (далее - министр), его заместители и уполномоченные должностные лица, определенные приказом Министерства, обеспечивают защиту персональных данных от неправомерного использования или утраты. Перечень персональных данных, обрабатываемых и хранимых в Министерстве, приводится в приложении к настоящему Положению.

5. Министр определяет лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Министерстве и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

6. Доступ к персональным данным без специального разрешения имеют министр и следующие государственные гражданские служащие Министерства:

заместители министра;

начальник управления бухгалтерского учета и бюджетного планирования;

начальник отдела и государственные гражданские служащие отдела бухгалтерского учета и отчетности;

начальник отдела и государственные гражданские служащие отдела организационной и кадровой работы;

начальник отдела правового регулирования и внутреннего аудита.

7. Оператор вправе обрабатывать персональные данные субъектов персональных данных только с их письменного согласия. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом

Согласия субъектов персональных данных не требуется в случаях, установленных федеральными законами.

8. Все персональные данные предоставляются субъектами персональных данных в установленном порядке лично. Если персональные данные возможно получить только у третьей стороны, то оператор обязан заранее уведомить об этом субъекта персональных данных и получить его письменное согласие.

9. Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

10. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его политических, религиозных и иных убеждениях и частной жизни без его письменного согласия.

11. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

12. При принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на сведениях, полученных исключительно в результате автоматизированной обработки или с использованием электронных носителей.

13. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных субъекта персональных данных с момента такого обращения или получения запроса на период проверки.

В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязан уточнить персональные данные и снять блокирование.

В случае подтверждения факта неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с момента выявления, обязан устранить допущенные нарушения либо при невозможности устранения допущенных нарушений уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

Уполномоченным органом по защите прав субъектов персональных данных является Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике

Дагестан (Управление Роскомнадзора по Республике Дагестан).

14. Оператор обязан обеспечить конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных.

15. Передача персональных данных третьей стороне не допускается без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральными законами.

16. В случае, если оператор поручает обработку персональных данных подведомственному учреждению, существенным условием выполнения работ является обязанность обеспечения указанным учреждением конфиденциальности персональных данных и безопасности персональных данных при их обработке.

17. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, за исключением случаев, установленных федеральными законами. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, а также при необходимости уничтожения или обезличивания части персональных данных указанные данные копируются и (или) уничтожаются в установленном порядке уполномоченными должностными лицами. Персональные данные, зафиксированные на материальном носителе, должны храниться в помещении, оборудованном специальными шкафами и сейфами, которые запираются и опечатываются.

18. В целях обеспечения защиты персональных данных субъекты персональных данных имеют право:

1) получать полную информацию о своих персональных данных и обработке персональных данных, в том числе автоматизированной;

2) осуществлять право свободного бесплатного доступа к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами;

3) требовать исключения или исправления неверных или неполных персональных данных, а также персональных данных, обработанных с нарушением федеральных законов. При отказе оператора исключить или исправить его персональные данные субъект персональных данных имеет право заявить в письменной форме в уполномоченный орган по защите прав субъектов персональных данных о своем несогласии, обосновав соответствующим образом такое несогласие;

4) требовать от оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных изменениях или исключениях;

5) обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном

порядке, если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований федеральных законов или иным образом нарушает его права и свободы.

19. Исключение возможности несанкционированного доступа к персональным данным обеспечивается:

1) раздельным хранением персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

2) запретом доступа к персональным данным (материальным носителям) без специального разрешения руководства Министерства иным лицам, кроме указанных в пункте 6 настоящего Положения;

3) хранением материальных носителей в специальных шкафах, сейфах, использованием паролей при обработке и хранении персональных данных в информационных системах в электронной форме;

4) запретом нахождения посторонних лиц в служебных помещениях Министерства, в которых располагаются соответствующие шкафы, сейфы, персональные компьютеры.

Реализация указанных мер осуществляется должностными лицами, уполномоченными на обработку персональных данных.

20. Должностные лица Министерства, уполномоченные на обработку и хранение персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за разглашение конфиденциальных сведений, содержащихся в персональных данных, а также за иные нарушения порядка обработки и хранения персональных данных, установленного настоящим Положением.

21. Ответственный за организацию обработки персональных данных в Министерстве назначается министром из числа государственных служащих, относящихся к высшей или главной группе должностей категории "руководители".

22. Ответственный за обработку персональных данных Министерства в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

23. Ответственный за обработку персональных данных Министерства обязан:

23.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Министерстве, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

23.2. осуществлять внутренний контроль за соблюдением государственными служащими Министерства требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

23.3. доводить до сведения государственных служащих Министерства положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

23.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Министерстве;

23.5. в случае нарушения в Министерстве требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

24. Ответственный за обработку персональных данных вправе:

24.1. иметь доступ к информации, касающейся обработки персональных данных в центральном аппарате Министерства и включающей:

24.1.1. цели обработки персональных данных;

24.1.2. категории обрабатываемых персональных данных;

24.1.3. категории субъектов, персональные данные которых обрабатываются;

24.1.4. правовые основания обработки персональных данных;

24.1.5. перечень действий с персональными данными, общее описание используемых в Министерстве способов обработки персональных данных;

24.1.6. описание мер, предусмотренных статьями 18.1 и 19 Федерального закона "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

24.1.7. дату начала обработки персональных данных;

24.1.8. срок или условия прекращения обработки персональных данных;

24.1.9. сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

24.1.10. сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

24.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Министерстве, иных государственных служащих с возложением на них соответствующих обязанностей и закреплением ответственности.

25. Ответственный за обработку персональных данных в Министерстве несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Министерстве в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение
к Положению об обработке персональных данных в Министерстве по физической культуре и спорту Республики Дагестан

ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ И ХРАНИМЫХ В МИНИСТЕРСТВЕ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ И СПОРТУ РЕСПУБЛИКИ ДАГЕСТАН

Наименование персональных данных	Основания для обработки	Содержание сведений
1. Персональные данные гражданских служащих (работников) Министерства, руководителей подведомственных учреждений находящихся в ведении Министерства и лиц претендующих на замещение соответствующих должностей	Трудовой кодекс Российской Федерации, Закон Республики Дагестан от 12 октября 2005 года N 32 "О государственной гражданской службе Республики Дагестан", Указ Президента РФ от 1 февраля 2005 г № 112 «Об утверждении Положения о конкурсе на замещение вакантной должности государственной гражданской службы РФ»	Фамилия, имя, отчество, дата и место рождения, гражданство, ИНН, СНИЛС, пол, знание иностранного языка, образование, профессия, сведения о трудовой деятельности, состояние в браке, состав семьи, номер паспорта, дата и место его выдачи, место жительства и дата регистрации, сведения о воинском учете, медицинское заключение, дополнительные сведения. Другие ведения, предусмотренные унифицированной формой N Т-2
2. База данных системы "1С: зарплата и кадры"		Фамилия, имя, отчество, дата рождения, серия и номер паспорта, дата и место его выдачи, адрес места проживания, СНИЛС, ИНН
3. Республиканский банк данных спортсменов Республики Дагестан, проходящих спортивную подготовку.	Федеральный закон от 4 декабря 2007 г № 329-ФЗ «О физической культуре и спорте в Российской Федерации», Закон Республики Дагестан от 2 февраля 2010 года № 5 «О физической культуре и спорте в Республике Дагестан»	Фамилия, имя, отчество, пол, дата рождения, принадлежность к физкультурно-спортивной организации, выбранный вид спорта, сведения о присвоении спортивных разрядов и званий, результаты спортивных достижений, сведения о спортивной дисквалификации, сведения о наградах, фамилия, имя, отчество тренера.

Приложение к приказу
Министерства по физической культуре
и спорту Республики Дагестан

от «01» 04 2013г № 77

Положение
о работе с персональными данными в информационной системе персональных данных

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а

также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

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

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

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.

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

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

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

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Положение об обеспечении безопасности персональных данных в Министерстве по физической культуре и спорту Республики Дагестан (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

2.2 Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных в Министерстве по физической культуре и спорту Республики Дагестан (далее – Министерство).

2.3 Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, а именно:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Постановления Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказа ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

2.3.1 Нормативных актов ФСТЭК России:

- «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15 февраля 2008 г.;

- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Положения о методах и способах защиты информации в информационных системах персональных данных», утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58 (зарегистрированного в Минюсте РФ 19.02.2010 N 16456);

2.3.2 Нормативных актов ФСБ России:

- «Типовых требований 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», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622;
- «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

2.4 Настоящее Положение предназначено для всех работников Министерство, а также лиц, получающих временный доступ к обрабатываемым в Минситерстве ПДн на законном основании. Ознакомление с Положением осуществляется под роспись в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных.

2.5 Настоящее Положение вступает в силу с момента его утверждения министром и действует до замены его новым Положением.

2.6 Плановая актуализация настоящего Положения проводится не реже, чем два раза в год. Внеплановая актуализация проводится при возникновении одного из следующих условий:

1) изменение целей и/или состава обрабатываемых персональных данных;

2) возникновение условий существенно влияющих на процессы обработки персональных данных и не регламентированных настоящим документом;

3) по результатам контрольных мероприятий и проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;

4) при появлении новых требований к обеспечению безопасности ПДн со стороны российского законодательства и контролирующих органов исполнительной власти Российской Федерации.

2.7 Ответственным за пересмотр настоящее Положение и составление рекомендаций по изменению является Администратор информационной безопасности.

2.8 Внесение изменений в настоящее Положение производится на основании соответствующего приказа министра.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Министерство РД является оператором ПДн.

3.2 В Министерство осуществляется обработка ПДн следующих категорий субъектов ПДн: работников Министерство, клиентов (физических лиц и представителей юридических лиц), данные которых получены Министерством в процессе осуществления своей деятельности.

3.3 ПДн, обрабатываемые в Министерстве, цели и сроки их обработки указаны в Перечне персональных данных, обрабатываемых в Министерстве.

3.4 В Министерство обработка ПДн осуществляется с использованием средств автоматизации и без использования таких средств.

3.5 Сроки хранения ПДн определяются в соответствие со сроком действия договора с субъектом ПДн, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

4. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн, и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности ПДн;
- нейтрализации и/или парирования реализуемых угроз безопасности ПДн;
- ликвидации последствий реализации угроз безопасности ПДн.

4.2 Организация работ по обеспечению безопасности ПДн Министерство должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите ПДн в Министерство.

4.3 Задачи по приведению Министерство «в соответствие с требованиями законодательства Российской Федерации в области защиты ПДн возлагаются на специально создаваемую для этих целей комиссию.

4.5 В случаях, когда Министерство на основании договора поручает обработку ПДн другому лицу/сторонней организации, необходимо выполнить одно из следующих условий:

- в тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности ПДн;

- в случае невозможности или нецелесообразности изменения текста договора оформить дополнительное соглашение к договору или соглашение о конфиденциальности, в которых прописать обязанность обеспечения контрагентом конфиденциальности персональных данных и безопасности ПДн при их обработке.

4.6 Работы по приведению Министерством в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям:

обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн организации.

4.7 Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, осуществляющих неавтоматизированную обработку ПДн в Министерстве;

- информирование работников организации об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;

- учет и защита носителей ПДн;

- разграничение доступа к носителям ПДн;

- уничтожение ПДн.

4.8 Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Министерство, осуществляются в рамках системы защиты персональных данных ИСПДн (далее - СЗПДн),

развертываемой в ИСПДн в процессе ее создания или модернизации.

4.9 СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

4.10 Система защиты ПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн Министерства.

4.11 Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

4.12 Структура, состав и основные функции СЗПДн определяются в соответствии с классом ИСПДн и моделью угроз безопасности персональных данных при их обработке в ИСПДн.

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 В целях оценки уровня защищенности обрабатываемых в Министерстве ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн раз в год должен проводиться анализ изменений процессов защиты ПДн.

5.2 Анализ изменений проводится по следующим основным направлениям:

- перечень лиц (подразделений), участвующих в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень и объем обрабатываемых ПДн;
- цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожение ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача ПДн;
- перечень программно-технических средств, используемых для

обработки ПДн;

- конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- способы физического подключения и логического взаимодействия компонент ИСПДн, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- состав используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;
- перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн ;
- физические меры защиты ПДн, организация пропускного режима.

5.3 Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

5.4 В Министерстве должен вестись учет действий, совершаемых с персональными данными в ИСПДн сотрудниками Министерства.

5.5 Доступ к ПДн регламентируется Регламентом по допуску лиц к обработке персональных данных.

5.6 Лица, участвующие в обработке ПДн, должны быть проинформированы:

- о факте обработки ими ПДн – реализуется путем ознакомления лиц, обрабатывающих ПДн с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым в Министерством;
- о категориях обрабатываемых ПДн – реализуется путем ознакомления утвержденным Перечнем персональных данных, обрабатываемых в Министерством;
- о правилах осуществления обработки ПДн – реализуется путем ознакомления под роспись с организационно-распорядительной документацией Министерства, регламентирующей процессы обработки ПДн, в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных

5.7 Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ. В Министерстве должен вестись учет носителей ПДн.

5.8 Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной

информации.

5.9 Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

• при необходимости использования или распространения определенных ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн – например, копирование части страницы, содержащей ПДн, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;

• 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 – например, копирование только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги.

5.10 Должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором информационной безопасности.

5.11 В Министерстве Администратором информационной безопасности должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

5.12 При обработке ПДн, Организация, должна иметь возможность и средства для восстановления ПДн, при их модификации или уничтожении вследствие несанкционированного доступа к ним.

5.13 Должен быть определен перечень помещений, используемых для обработки ПДн. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.14 Пользователи ИСПДн должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя, пользователи должны немедленно сообщить об этом Администратору информационной безопасности.

5.15 Если при работе с ПДн работнику Министерство необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

5.16 В случае достижения цели обработки ПДн Организация прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства) и

уничтожает ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.17 Проведение работ по созданию (модернизации) СЗПДн Компании включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

5.18 На предпроектной стадии проводится классификация ИСПДн, формируется модель угроз безопасности ПДн при их обработке в ИСПДн, разрабатывается техническое задание на СЗПДн.

5.19 Классификация ИСПДн осуществляется в соответствии с положениями Приказа ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

5.20 В связи с тем, что в ИСПДн Министерство помимо обеспечения конфиденциальности обрабатываемых ПДн требуется обеспечить целостность и доступность ПДн, ИСПДн Министерствоа являются специальными информационными системами. ИСПДн Министерствоа указаны в Перечне информационных систем персональных данных Министерство.

5.21 Класс ИСПДн оформляется соответствующим актом.

5.22 Модель угроз безопасности ПДн при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

5.23 Перечень актуальных угроз формируется для каждой ИСПДн Министерство с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

5.24 По итогам классификации ИСПДн и результатам определения актуальных угроз безопасности ПДн формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

5.25 Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн, а именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания;

5.26 Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты

информации и их установку;

- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПДн и средства защиты информации.

5.27 На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

5.28 В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение класса ИСПДн;
- произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.).

5.29 Задачи по приведению ИСПДн Министерство в соответствие с требования законодательства РФ в области защиты ПДн возлагаются на Администратора информационной безопасности.

5.30 При возникновении условий влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности персональных данных и пр.) необходимо незамедлительно проинформировать об этом Администратора информационной безопасности.

5.31 Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.