УТВЕРЖДЕНО
приказом врио директора
ГАУ РД «МФЦ в РД»
Арсланалиева М.И.
от «28» 03 2023 г. № 92

ПОЛИТИКА

ГАУ РД «МФЦ в РД»

в области обработки и защиты персональных данных

1. Информация о документе

1.1. В целях поддержания деловой репутации и гарантирования выполнения норм федерального законодательства в полном объеме, ГАУ РД «МФЦ в РД» (далее – Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в ГАУ РД «МФЦ В РД» (далее – Политика) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных субъектов персональных данных.

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

1.3. Назначение документа

Настоящая политика информационной безопасности устанавливает статус, структуру, и сферы ответственности, а также цели, задачи и функции.

1.3.1. Доступ и периодичность пересмотра

Тип документа:	Политика
Аннотация:	Политика информационной безопасности
Периодичность пересмотра	1 года
Доступ:	Для внутреннего пользования

1.3.2. Контроль версий документа

Номер версии	Дата создания версии	Должность ответственного за разработку	ФИО ответственного за разработку	Краткое описание изменений
2.0	19.02.2018	Начальник отдела по защите информации	Бадрудинов Б.К.	Создание документа

2.Общие положения

2.1. Термины и определения:

2.1.1. *Автоматизированная система* – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.1.2. *Анализ риска* –систематическое использование информации для определения источников и оценки риска.

2.1.3. *Аудит информационной безопасности* – процесс проверки выполнения установленных требований по обеспечению информационной безопасности.

2.1.4. *Аутентификация* – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

2.1.5. *Доступ к информации* – возможность получения информации и ее использования.

2.1.6. *Защищенный канал передачи данных* – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

2.1.7. *Идентификатор доступа* – уникальный признак субъекта или объекта доступа.

2.1.8. *Идентификация* – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2.1.9. *Информация* – это актив, который, подобно другим активам ГАУ РД «МФЦ в РД», имеет ценность и, следовательно, должен быть защищен надлежащим образом.

2.1.10. *Информационная безопасность* – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов ГАУ РД «МФЦ в РД» в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов ГАУ РД «МФЦ в РД».

2.1.11. *Информационная система* – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ГАУ РД «МФЦ в РД». В ГАУ РД «МФЦ в РД» используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

2.1.12. *Информационные технологии* – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.1.13. *Информационные активы* – информационные системы, информационные средства, информационные ресурсы.

2.1.14. *Информационные средства* – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

2.1.15. *Информационные ресурсы* – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

2.1.16. *Инцидент информационной безопасности* – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов ГАУ РД «МФЦ в РД».

2.1.17. *Источник угрозы* – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

2.1.18. *Конфиденциальная информация* – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

2.1.19. *Конфиденциальность* – доступ к информации только авторизованных пользователей.

2.1.20. *Критичная информация* – информация, нарушение доступности, целостности, либо конфиденциальности, которой может оказать негативное влияние на функционирование подразделений ГАУ РД «МФЦ в РД», привести к причинению ГАУ РД «МФЦ в РД» материального или иного вида ущерба.

2.1.21. *Локальная вычислительная сеть (ЛВС)* – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

2.1.22. *Мониторинг информационной безопасности* – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы ГАУ РД «МФЦ в РД», информационные услуги ГАУ РД «МФЦ в РД» и пр.

2.1.23. *Несанкционированный доступ к информации (НСД)* – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

2.1.24. *Обработка риска* – процесс выбора и осуществления мер по модификации риска.

2.1.25. *Остаточный риск* – риск, остающийся после обработки риска.

2.1.26. *Политика информационной безопасности* – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

2.1.27. *Пользователь ЛВС* – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

2.1.28. *Программное обеспечение* – совокупность прикладных программ, установленных на сервере или ЭВМ.

2.1.29. *Рабочая станция* – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

2.1.30. *Регистрационная (учетная) запись пользователя* – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

2.1.31. *Роль* – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

2.1.32. *Собственник* – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

2.1.33. *Угрозы информационным данным* – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или

модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

2.1.34. *Управление информационной безопасностью* – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

2.1.35. *Уязвимость* – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности ГАУ РД «МФЦ в РД» при реализации угроз в информационной сфере.

2.1.36. *Целостность информации* – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

2.1.37. *ЭВМ* – электронная - вычислительная машина, персональный компьютер.

2.1.38. *Электронная цифровая подпись* – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

3. Информация об операторе

Наименование: **Государственное автономное учреждение Республики Дагестан «Многофункциональный центр предоставления государственных и муниципальных услуг в Республике Дагестан»**.

Сокращенное наименование: **ГАУ РД «МФЦ в РД»**.

ИНН: **0572004299/055401001**

Фактический адрес: Россия, 367000, Республика Дагестан, город Махачкала, пр.

Насрутдинова, д.1.

Тел./факс: **8 (8722) 51-11-15**

Реестр операторов персональных данных: http://rkn.gov.ru/personal-data/register/?id=5-14-000612 , **5-14-000612**, Приказ № 161 от 16.05.2014г.

4. Правовые основания обработки персональных данных

4.1. Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

4.1.1. Конституцией Российской Федерации.

4.1.2. Трудовым кодексом Российской Федерации.

4.1.3. Гражданским кодексом Российской Федерации.

4.1.4. Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

4.1.5. Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

4.1.6. Федеральным законом от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4.1.7. Федеральным законом от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

4.1.8. Федеральным законом от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

4.1.9. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

4.1.10. Постановление Правительства РФ 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».

4.1.11. Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной

службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

4.1.12. Постановление Правительства РФ от 06.07.2008 № 512 «Об Утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

4.1.13. Постановление Правительства РФ от 15.09.2008 № 687 «Об Утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.1.14. Постановлением Правительства РФ от 15.09.1993 №912-51 «О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам».

4.1.15. Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об Утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.16. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4.1.17. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.1.18. Приказ ФСТЭК России от 11.02.2013 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспертному контролю».

4.1.19. Приказ ФСТЭК России от 23.03.2017 г. № 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в требования к обеспечению защиты

информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

4.1.20. Приказ Минкомсвязи России от 14.11.2011 № 312 «Об утверждении административного регламента исполнения федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных».

4.1.21. Приказ ФСБ России № 416, ФСТЭК России № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

4.1.22. Приказ Роскомнадзора № 996 от 5.09.2013 «Об утверждении требований и методов по обезличиванию персональных данных».

4.2. Во исполнение настоящей Политики руководящим органом Оператора утверждены следующие локальные нормативные правовые акты:

4.2.1. Положение об обработке персональных данных.

4.2.2. Перечень обрабатываемых персональных данных

4.2.3. Перечень информационных систем персональных данных.

4.2.4. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

4.2.5. Инструкция о порядке обработки персональных данных без использования средств автоматизации.

5. Цели обработки персональных данных

5.1. Оператор обрабатывает персональные данные исключительно в следующих целях:

7.2. Оператор осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

7.3. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

7.4. Оператором созданы общедоступные источники персональных данных (справочники). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, должность, абонентский номер, адрес корпоративной электронной почты), включаются в такие источники только с письменного согласия субъекта персональных данных.

7.5. Оператор осуществляет обработку ПДн с использованием ИСПДН второго класса защищенности.

8. Сведения о третьих лицах, участвующих в обработке персональных данных

8.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

8.1.1. Федеральной налоговой службе.

8.1.2. Пенсионному фонду России.

8.1.3. Негосударственным пенсионным фондам.

8.1.4. Филиалам ГАУ РД «МФЦ В РД».

8.1.5. Участникам Системы межведомственного электронного взаимодействия.

8.1.6. Кредитным организациям.

8.1.7. Лицензирующим и контролирующим органам государственной власти и местного самоуправления.

8.1.8. Саморегулируемым организациям.

8.2. Оператор поручает обработку персональных данных другим лицам на основании договора «О предоставлении услуг».

9. Меры по обеспечению безопасности персональных данных при их обработке

9.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

9.1.1. Назначением ответственных за организацию обработки персональных данных.

9.1.2. Осуществлением внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

9.1.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных сотрудников.

9.1.4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

8.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

9.1.6. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

9.1.7. Учетом физических носителей персональных данных.

9.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

9.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9.1.11. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

9.2. Обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются в «Положении об обработке персональных данных в ГАУ РД «МФЦ В РД» (см.п.3.2.1).

10. Права субъектов персональных данных

10.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

10.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

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

10.3.1. Если обработка персональных данных, включая те, что получены в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, выполняется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка.

10.3.2. При условии, что обработка персональных данных производится органами,

осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившим и к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными.

10.3.3. Если обработка персональных данных выполняется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

10.3.4. Когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

10.3.5. Если 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.

10.4. Для реализации своих прав (см.пп.9.1–9.3) и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

10.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных (см.п.11.2).

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

11. Контактная информация

11.1. Ответственным за организацию обработки и обеспечения безопасности персональных данных в ГАУ РД «МФЦ В РД» назначен специалист по защите информации Исаев Насрудин Русланович.

11.2. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Управление Роскомнадзора по Республике Дагестан:

Адрес: 367000, РД, г. Махачкала, ул. С.Стальского, 2.

Тел.: (8722) 68-26-00.

Тел.: (8722) 98-00-09.

Факс: (8722) 98-00-09.

E-mail: rsockanc05@rkn.gov.ru

Сайт: 05.rkn.gov.ru

12. Заключительные положения

12.1. Настоящая Политика разрабатывается отделом по защите информации, утверждается директором ГАУ РД «МФЦ в РД».

12.2. Срок действия настоящей Политики – один год с момента утверждения. По истечении срока действия (при необходимости–ранее) Политика подлежит пересмотру. Внесение изменений в Политику производит отдел по защите информации.

12.3. Настоящая Политика обязательна для соблюдения и подлежит доведению до всех сотрудников Учреждения. Контроль за соблюдением Политики осуществляет директор ГАУ РД «МФЦ в РД».

Начальник отдела по защите информации Бадрудинов Б.К.

Согласовано:

Начальник юридического отдела Абдулжелилов А. А.

Начальник отдела кадров Зайнутдинова Ф.Б.

ЛИСТ ОЗНАКОМЛЕНИЯ

с Политикой в отношении обработки персональных данных

№ п/п	Должность	Фамилия, инициалы	Подпись, дата
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

5.1.1. Исполнения положений нормативных актов, указанных в п.3.1.

5.1.2. Принятия решения о трудоустройстве кандидата в ГАУ РД «МФЦ В РД».

5.1.3. Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.

5.1.4. Осуществления пропускного и внутриобъектового режима Оператора.

5.1.5. Предоставления государственных, муниципальных и дополнительных (сопутствующих) услуг.

6. Категории обрабатываемых персональных данных, источники их получения, сроки обработки и хранения

6.1. В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных:

6.1.1. Персональные данные сотрудников. Источники получения: субъекты персональных данных ГАУ РД «МФЦ В РД».

6.1.2. Персональные данные учредителей, генерального директора, аффилированных лиц Учреждения. Источники получения: субъекты персональных данных ГАУ РД «МФЦ В РД».

6.1.3. Персональные данные посетителей. Источники получения: субъекты персональных данных - посетители.

6.1.4. Персональные данные кандидатов. Источники получения: субъекты персональных данных - кандидаты на должность.

6.2. Сроки обработки и хранения персональных данных определены в «Положение об обработке персональных данных в ГАУ РД «МФЦ В РД».

7. Основные принципы обработки, передачи и хранения персональных данных

7.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона 152-ФЗ «О персональных данных».