Приложение
к приказу департамента
социальной защиты
Воронежской области
от «28» июня 2018 г.
№ 1346/ОД

Политика информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области

Оглавление

Введение

Настоящая политика информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в концепции информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области.

Основной целью Политики является обеспечение безопасности объектов защиты органов социальной защиты населения Воронежской области от всех видов угроз безопасности персональных данных.

1. Основные понятия и термины, используемые в настоящем документе

В настоящем документе используются следующие основные понятия и термины и их определения:

Автоматизированное рабочее место - рабочее место пользователя в составе комплекса средств автоматизации.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью работников, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных и без использования средств автоматизации.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Конфиденциальная информация – требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации.

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.

Материальный носитель – изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.

Несанкционированный доступ к информации (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие установленные правила разграничения доступа.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Объект защиты – персональные данные, информация, обрабатываемая в информационных системах персональных данных, технические средства обработки и защиты персональных данных.

Органы социальной защиты населения Воронежской области – департамент социальной защиты Воронежской области, государственные учреждения, в отношении которых департамент социальной защиты Воронежской области исполняет функции и полномочия учредителя.

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. В настоящем документе операторами являются департамент социальной защиты населения Воронежской области и подведомственные ему учреждения.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2. Правовая основа

Основой для разработки настоящей Политики служат требования:

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

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Трудового кодекса Российской Федерации;

– 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»;

– постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– постановления правительства Воронежской области от 26 сентября 2017 г. № 748 «Об утверждении документов, определяющих политику в отношении обработки персональных данных в правительстве Воронежской области»;

– методических документов ФСБ России, ФСТЭК России, Роскомнадзора;

– иных нормативных правовых актов в сфере защиты информации.

3. Область применения

Настоящая Политика распространяется на все учреждения системы социальной защиты населения Воронежской области, которая включает в себя департамент социальной защиты Воронежской области (далее – Департамент), государственные учреждения, в отношении которых Департамент исполняет функции и полномочия учредителя (далее – подведомственные учреждения).

Требования настоящей Политики носят обязательный характер для всех работников учреждений социальной защиты населения (штатных, временных, работающих по контракту и т.п.), имеющих доступ к персональным данным граждан, включая персональные данные самих работников.

Требования Политики распространяются на порядок и условия обработки персональных данных в органах социальной защиты населения Воронежской области с использованием средств автоматизации и без использования таких средств.

Настоящая Политика является методологической основой для разработки следующих документов:

– частные модели угроз безопасности персональных данных при их обработке в информационных системах;

– акты классификации информационных систем персональных данных;

– положение (правила) обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение

нарушений законодательства Российской Федерации в сфере персональных данных;

– положение о разрешительной системе доступа к персональным данным;

– перечень информационных систем персональных данных;

– перечни персональных данных, обрабатываемых в органах социальной защиты населения области в связи с реализацией трудовых отношений, а также в связи с оказанием социальных услуг, социальной поддержки;

– перечень должностей служащих Департамента, подведомственных учреждений, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– типовая форма обязательства работника, непосредственно осуществляющего обработку персональных данных, в случае увольнения прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

– типовая форма согласия на обработку персональных данных работников органов социальной защиты населения области, иных субъектов персональных данных;

– типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

– порядок доступа работников в помещения, в которых ведется обработка персональных данных.

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

Обработка персональных данных в органах социальной защиты населения осуществляется на законной и справедливой основе.

Органы социальной защиты населения Воронежской области устанавливают следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

– издание правовых актов (приказов) по вопросам обработки и защиты персональных данных;

– назначение ответственных за организацию обработки и обеспечение безопасности персональных данных;

– определение сотрудников, допущенных к обработке (получение, хранение, передача и т.д.) (далее - обработка) персональных данных в учреждении и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных;

– ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, под роспись до начала работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

– получение персональных данных лично у субъекта персональных данных, в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных, в случае возникновения необходимости получения персональных данных у третьей стороны учреждение извещает об этом субъекта персональных данных заранее, получает его письменное согласие и сообщает ему о целях, предполагаемых источниках и способах получения персональных данных;

– применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

– опубликование на официальном сайте учреждения в информационно-телекоммуникационной сети Интернет документов, определяющих политику учреждения в отношении обработки персональных данных, реализуемые требования к защите персональных данных;

– осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике учреждения в отношении обработки персональных данных, локальным актам учреждения.

5. Обработка персональных данных

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.

Система обработки информации – совокупность средств и методов получения и преобразования информации, позволяющая на основе исходного массива данных получить совокупность выходных показателей, необходимых для анализа, контроля, планирования, управления.

Обработка персональных данных без использования средств автоматизации включает в себя любые действия с персональными данными, размещенными на материальных носителях, осуществляемую человеком.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации

(неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных, либо были извлечены из нее.

Обработка персональных данных в информационных системах представляет собой обработку персональных данных, содержащихся в базах данных с использованием информационных технологий и технических средств.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

5.1. Цели обработки персональных данных в органах социальной защиты населения Воронежской области

Обработка персональных данных в органах социальной защиты населения Воронежской области осуществляется в целях исполнения полномочий по социальному обслуживанию и социальной поддержке

граждан, определенными федеральными и региональными нормативными правовыми актами, а также ведения кадровой работы и бухгалтерского учета.

5.2. Принципы работы с персональными данными

Обработка персональных данных осуществляется на основе принципов:

1. Обработка персональных данных осуществляется на законной и справедливой основе.

2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому

является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.3. Состав персональных данных

Состав (объем и содержание) персональных данных определяется нормативными правовыми актами, устанавливающими порядок предоставления мер социальной поддержки, социального обслуживания, кадрового, бухгалтерского учета, иными документами, регламентирующими порядок осуществления функций органов социальной защиты населения Воронежской области. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных полномочий.

5.4. Категории субъектов, персональные данные которых обрабатываются в органах социальной защиты населения Воронежской области

К категориям субъектов, персональные данные которых обрабатываются в органах социальной защиты населения Воронежской области, относятся:

- государственные гражданские служащие Департамента;
- работники, замещающие в Департаменте должности, не являющиеся должностями государственной гражданской службы;
- работники подведомственных Департаменту учреждений;
- кандидаты на замещение вакантных должностей и на включение в кадровый резерв Департамента;

- граждане, обратившиеся в органы социальной защиты населения Воронежской области в целях получения мер социальной поддержки, социального облуживания.

5.5. Сроки обработки и хранения персональных данных

Персональные данные, связанные с реализацией трудовых отношений, обрабатываются и хранятся в течение срока действия служебного контракта (трудового договора) и в течение 75 (семидесяти пяти) лет после его прекращения.

Персональные данные, связанные с предоставлением мер социальной поддержки, социального обслуживания, обрабатываются и хранятся до достижения цели их обработки, в соответствии с правилами бухгалтерского учета и в соответствии с Перечнем типовых документов, образующихся в деятельности госкомитетов, министерств, ведомств и других учреждений, организаций, предприятий, с указанием сроков хранения», утвержденным начальником Главного архивного управления при Совете Министров СССР 15.08.1988 (в редакциях от 06.10.2000, от 31.07.2007).

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

В случае достижения цели обработки персональных данных обработка персональных данных оператором прекращается, персональные данные уничтожаются в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральным законодательством.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных их обработка оператором прекращается, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, персональные данные уничтожаются в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено служебным контрактом, договором или соглашением, стороной которого является субъект персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

Уничтожение носителей персональных данных, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения, утверждаемого руководителем оператора.

Решение об удалении(стирании) записей, содержащих персональные данные, в электронных базах данных принимается сотрудниками, допущенными к обработке персональных данных самостоятельно в срок, не превышающий тридцати дней по достижении целей обработки или с момента утраты необходимости в достижении этих целей.

Сведения, содержащие персональные данные, и относимые к архивным документам, образующимся в процессе деятельности органов социальной защиты населения Воронежской области, включаются в состав электронных архивов и хранятся согласно установленным законодательством срокам отдельно от баз данных информационных систем органов социальной защиты населения Воронежской области.

5.7. Правила работы с обезличенными персональными данными

Обезличивание персональных данных в органах социальной защиты населения Воронежской области проводится с целью снижения ущерба от разглашения персональных данных, снижения класса защищенности

информационных систем персональных данных и по достижении целей обработки персональных данных или утраты необходимости в достижении этих целей.

Способы обезличивания персональных данных:

- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- деление сведений на части и обработка в разных информационных системах.

Решение о необходимости обезличивания персональных данных принимает руководитель учреждения.

Ответственный за обеспечение безопасности персональных данных готовит предложения по обезличиванию персональных данных, обоснование такой необходимости и способы обезличивания.

Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом оператора.

Контроль за соблюдением порядка обезличивания персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в рамках внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных.

5.8. Условия обработки персональных данных

Обработка персональных данных осуществляется оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных федеральным законодательством.

В случае, если в рамках действующего законодательства и в целях реализации своих полномочий оператор на основании договора (соглашения) осуществляет передачу или получение персональных данных от другого

лица, существенным условием договора (соглашения) должна являться обязанность обеспечения сторонами договора (соглашения) конфиденциальности персональных данных и безопасности персональных данных при их обработке.

5.9. Согласие субъекта персональных данных на обработку своих персональных данных

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В связи с заявительным принципом предоставления мер социальной поддержки и социального обслуживания согласие субъекта персональных данных на обработку своих персональных данных в целях получения социальной поддержки, социального обслуживания включается в состав заявления гражданина или его законного представителя.

Типовая форма согласия на обработку персональных данных работников органов социальной защиты населения приведена в приложении 1 к настоящей Политике.

В случае отказа гражданином предоставить персональные данные, утвержденные порядками предоставления мер социальной поддержки или социального обслуживания, или в согласии на их обработку оператор обязан разъяснить субъекту персональных данных юридические последствия такого отказа.

5.10. Правила рассмотрения запросов субъектов персональных данных или их представителей

Субъекты персональных данных или их законные представители в

соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и способы обработки персональных данных;

4) наименование и место нахождения Департамента (подведомственного учреждения);

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

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

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

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

Субъекты персональных данных вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Указанные сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя, содержащего:

1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2) сведения, подтверждающие участие субъекта персональных данных в правоотношениях (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных;

3) подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Департамент (или подведомственное учреждение) обязано сообщить в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или

персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Департамент (или подведомственное учреждение) обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

Департамент (или подведомственное учреждение)обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Департамент (или подведомственное учреждение) обязано уничтожить такие персональные данные. Департамент (или подведомственное учреждение) обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

В случае если сведения, а также обрабатываемые персональные данные, были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе повторно обратиться в

Департамент (или подведомственное учреждение)лично или направить повторный запрос в целях получения сведения и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством Российской Федерации или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе повторно обратиться Департамент (или подведомственное учреждение) лично или направить повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения указанного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в случаях, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Обращения субъектов персональных данных о соблюдении их законных прав регистрируются оператором в специальном журнале. Форма журнала приведена в приложении 2 к настоящей Политике.

6. Обеспечение безопасности персональных данных

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Основными направлениями обеспечения безопасности персональных данных являются:

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

б) обеспечение своевременного обнаружения фактов несанкционированного доступа к персональным данным;

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

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

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

6.1. Организационная структура управлением информационной безопасности

В целях эффективного управления системой защиты персональных данных органов социальной защиты населения Воронежской области, своевременного реагирования на изменения в информационной структуре, существенно влияющих на установленные уровни безопасности информации, в Департаменте создается нештатное подразделение по защите информации – комиссия по обеспечению безопасности персональных данных (далее – Комиссия). В состав комиссии входят:

– председатель Комиссии, назначаемый из числа заместителей руководителя Департамента;

– заместитель председателя Комиссии– сотрудник службы управления персоналом Департамента, отвечающий за планирование и контроль

выполнения организационных мероприятий по безопасности информации и персональных данных;

– заместитель председателя Комиссии – сотрудник службы информационных технологий, отвечающий за планирование и организацию мероприятий по обеспечению безопасности информации и персональных данных в информационных системах;

– члены Комиссии – сотрудники структурных подразделений Департамента и подведомственных учреждений.

В целях реализации мероприятий по обеспечению безопасности персональных данных в Департаменте и во всех подведомственных учреждениях назначаются ответственные лица.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации приказом руководителя назначаются должностные лица, ответственные за обеспечение безопасности персональных данных с учетом классификации персональных данных. В частности, ответственным за безопасность персональных данных работников назначается работник кадровой службы, ответственным за безопасность персональных данных, обрабатываемых в бухгалтерской службе, назначается работник бухгалтерской службы.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах приказом руководителя должны быть назначены ответственные за обеспечение безопасности персональных данных:

1. В информационных системах, предназначенных для обработки персональных данных граждан в целях предоставления социальной поддержки, социального обслуживания:

– в Департаменте– работники отдела развития информационных ресурсов;

– в подведомственных учреждениях –работники учреждений;

2. В информационных системах, предназначенных для обработки персональных данных сотрудников органов социальной защиты населения в целях осуществления кадрового учета, – работники кадровой службы.

3. В информационных системах, предназначенных для обработки персональных данных сотрудников органов социальной защиты населения в целях осуществления бухгалтерского учета, – работники бухгалтерской службы.

Общее руководство работами по обеспечению безопасности персональных данных в органах социальной защиты населения осуществляет председатель комиссии. Непосредственное руководство и контроль за обеспечением безопасности персональных данных возлагается на заместителей председателя комиссии.

Руководство организацией работ по обеспечению информационной безопасности в подведомственных учреждениях осуществляет руководитель этого учреждения.

Сотрудники структурных подразделений Департамента и подведомственных учреждений, ответственные за вопросы обеспечения безопасности персональных данных в своих подразделениях, организуют планирование и контроль выполнения мероприятий по защите персональных данных в подразделениях.

Должностные лица подведомственных учреждений, ответственные за обеспечение безопасности персональных данных при их обработке в информационных системах, осуществляют свою деятельность под методическим руководством и по согласованию с Комиссией, должностными лицами Департамента, ответственными за обеспечение безопасности персональных данных в соответствующих информационных системах.

6.1.1. Деятельность Комиссии по обеспечению безопасности персональных данных

Комиссия Департамента по обеспечению безопасности персональных данных наделяется следующими полномочиями:

1. Организация составления и контроль выполнения планов по обеспечению информационной безопасности в органах социальной защиты населения области Воронежской области.

2. Разработка предложений по изменению политики информационной безопасности Департамента и подведомственных учреждений.

3. Разработка нормативных правовых актов и иных документов, регламентирующих деятельность по обеспечению информационной безопасности в органах социальной защиты населения Воронежской области.

4. Определение требований к мерам обеспечения информационной безопасности.

5. Методическое руководство деятельностью по обеспечению информационной безопасности в подведомственных учреждениях.

6. Контроль выполнения требований документов, регламентирующих деятельность по обеспечению информационной безопасности в органах социальной защиты населения Воронежской области, работниками Департамента.

7. Участие в расследовании событий, связанных с инцидентами информационной безопасности. При необходимости внесение предложений по применению санкций в отношении лиц, осуществивших несанкционированный доступ и нерегламентированные действия с персональными данными, нарушивших требования документов, инструкций по обеспечению информационной безопасности.

Работники подведомственных учреждений, ответственные за обеспечение безопасности персональных данных, осуществляют свою деятельность под методическим руководством Комиссии. В число их обязанностей входят:

– организация выполнения мероприятий по обеспечению информационной безопасности в учреждении;

– контроль выполнения требований документов, регламентирующих деятельность по обеспечению информационной безопасности в органах социальной защиты населения Воронежской области, работниками учреждения;

– мониторинг событий, связанных с обеспечением информационной безопасности.

6.1.2. Должностные обязанности лица, ответственного за организацию обработки персональных данных

В обязанности лица, ответственного за обработку персональных данных в Департаменте (подведомственного учреждения), входит:

- организовывать и контролировать разработку проектов правовых актов (приказов) по вопросам обработки персональных данных;

- осуществлять контроль за соблюдением процедур, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, устранение последствий таких нарушений;

- обеспечивать доведение до сведения лиц, непосредственно осуществляющих обработку персональных данных, положения законодательства Российской Федерации в области персональных данных (в том числе о требованиях к защите персональных данных) и (или) обеспечивать организацию обучения указанных работников;

- обеспечивать уведомление уполномоченного органа по защите прав субъектов персональных данных о намерении Департамента (подведомственного учреждения)осуществлять обработку персональных данных, изменении сведений, указанных в уведомлении, или о прекращении обработки персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

- в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям законодательства Российской Федерации в области персональных данных организовывать проведение проверок, в том числе:

- обеспечивать разработку, представление на утверждение руководителю Департамента (директору подведомственного учреждения) ежегодного плана внутреннего контроля 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, правовым актам Департамента;

- по результатам проведенной проверки представлять губернатору Воронежской области заключение о результатах проведенных проверок и мерах, необходимых для устранения выявленных нарушений.

За ненадлежащее исполнение или неисполнение возложенных должностных обязанностей, связанных с выполнением требований законодательства Российской Федерации в области персональных данных, ответственный за организацию обработки персональных данных несет ответственность, предусмотренную законодательством Российской Федерации.

6.2. Организационные меры обеспечения безопасности персональных данных, связанные с персоналом

Перечень должностей работников Департамента (подведомственного учреждения), допущенным к персональным данным, другой конфиденциальной информации, утверждается правовым актом руководителя Департамента (директора подведомственного учреждения).

Все работники, имеющие доступ к персональным данным, обязаны знать и строго выполнять установленные правила и обязанности по доступу к персональным данным и соблюдению режима безопасности персональных данных.

Лица, осуществляющие обработку персональных данных, информируются о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами Российской Федерации, федеральных органов исполнительной власти, органов исполнительной власти Воронежской области, настоящим документом.

Обязанности по соблюдению требований безопасности включаются в трудовые договоры (служебные контракты).

Все работники, осуществляющие обработку персональных данных, имеющие к ним доступ в целях осуществления служебных обязанностей, берут на себя обязательство о конфиденциальности (неразглашении) информации. Типовая форма обязательства приведена в приложении 3 к настоящей Политике.

Функции (роли) и ответственность в области информационной безопасности документируются. Выполнение должностных обязанностей, связанных с обработкой персональных данных, отражается в должностных инструкциях (должностных регламентах).

При вступлении в должность нового сотрудника непосредственный руководитель подразделения, в которое он поступает, организует его ознакомление с необходимыми документами, регламентирующими требования по защите персональных данных, настоящим документом, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования персональных данных.

Получение специалистами информации о выполнении должностных обязанностей, связанных с обработкой персональных данных, о

необходимости соблюдения их конфиденциальности и режима безопасности персональных данных, оформляется в письменном виде.

6.3. Требования к персоналу

Лица, допущенные к персональным данным, другой конфиденциальной информации, обязаны:

– не сообщать конфиденциальную информацию лицам, не имеющим права доступа к ней;

– обеспечивать сохранность материальных носителей с конфиденциальной информацией;

– не делать неучтенных копий на бумажных и электронных носителях;

– не оставлять включенными персональные компьютеры с предоставленными правами доступа в информационные системы персональных данных, не оставлять материалы с конфиденциальной информацией на рабочих столах. После окончания работы (в перерывах) покидая рабочее место, сотрудник обязан убрать документы и электронные носители с конфиденциальной информацией в закрываемые на замок сейфы, шкафы, столы, и т.п.;

– при работе с документами, содержащими конфиденциальную информацию, исключать возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;

– не выносить документы и иные материальные носители с конфиденциальной информацией, а также их копии из служебных помещений, предназначенных для работы с ними;

– немедленно сообщать непосредственному руководителю о недостаче, утрате, утечке или искажении конфиденциальной информации, об обнаружении неучтенных материалов с указанной информацией;

– не допускать действий, способных повлечь утечку конфиденциальной информации.

6.4. Использование ресурсов сети Интернет

Подключение информационных систем персональных данных к сетям общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сети), не допускается.

При необходимости подключения средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных и другой конфиденциальной информации, к сетям общего доступа и (или) международного обмена (сети Интернет и других)такое подключение должно производиться только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю Российской Федерации.

Решение об использовании сети Интернет для служебной и (или) собственной хозяйственной деятельности принимается руководителем учреждения. При этом цели использования сети Интернет должны быть явно перечислены.

Решение об организации доступа к сети Интернет на конкретных компьютерах принимается руководителем оператора на основании сведений, представленных руководителем структурного подразделения, и согласованных с лицом, ответственным за обеспечение информационной безопасности.

Взаимодействие с сетью Интернет в режиме «он-лайн» осуществляется на выделенных персональных компьютерах, изолированных физически или посредством межсетевого экранирования от внутренних сетей компьютеров, на которых осуществляется обработка персональных данных.

Почтовый обмен с сетью Интернет должен быть организован через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними.

Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к сетям общего доступа и (или) международного обмена (сети Интернет и других), не допускается.

При работе в сетях общего доступа и (или) международного обмена соблюдаются следующие правила:

1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) на элементах информационной системы проводится при служебной необходимости.

2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты;

– передавать по Сети защищаемую информацию без использования средств шифрования;

– скачивать из Сети программное обеспечение и другие файлы;

– посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое программное обеспечение и другие);

– нецелевое использование подключения к Сети.

6.5. Антивирусная защита

Антивирусная защита направлена на предотвращение угроз, связанных с воздействием вредоносного программного кода.

Основные принципы антивирусной защиты:

1. Антивирусное программное обеспечение устанавливается, настраивается и активируется на всех серверах, рабочих станциях и локальных персональных компьютерах, используемых специалистами органов социальной защиты населения Воронежской области.

2. Эксплуатация средств антивирусной защиты осуществляется только на основании лицензионных соглашений с их правообладателями.

3. Состав, архитектура и конфигурация системы антивирусной защиты стандартизованы.

4. Все возможные каналы поступления вредоносных программ в информационно-технологическую инфраструктуру органов социальной защиты населения Воронежской области подлежат определению, анализу и защите средствами антивирусной защиты.

5. Вся информация, создаваемая и обрабатываемая техническими средствами, а также принимаемая (передаваемая) посредством сменных носителей информации и средств телекоммуникаций подвергается контролю на предмет обнаружения вредоносных программ.

6. С целью эффективной борьбы с новыми видами вредоносных программ выполняется регулярное обновление всех средств антивирусной защиты.

7. Любые средства вычислительной техники, используемые в органах социальной защиты населения области, в ходе эксплуатации подвергаются непрерывному антивирусному мониторингу и сканированию.

6.6. Учет носителей информации

Во всех структурных подразделениях оператора, осуществляющих обработку персональных данных, организуется учет материальных носителей персональных данных (далее – защищаемые носители). Учет защищаемых носителей персональных данных осуществляется специально уполномоченными из числа сотрудников лицами.

Учет всех защищаемых носителей информации производится с помощью их маркировки и занесения учетных данных в «Журнал учета электронных носителей персональных данных» с отметкой об их движении(выдаче и возврате). С этой целью на защищаемых носителях персональных данных проставляются следующие реквизиты:

- регистрационный номер;
- дата и роспись уполномоченного лица.

Выдача защищаемых носителей персональных данных сотруднику производится под его личную роспись.

Листы журналов нумеруются, прошиваются и опечатываются.

6.7. Порядок хранения электронных носителей персональных данных

Хранение документов и информационных ресурсов, содержащих персональные данные и иную конфиденциальную информацию, в электронном виде осуществляется только на предварительно учтенных машиночитаемых (электронных) носителях.

Носители информации с персональными данными хранятся в служебных помещениях, в надежно запираемых и опечатываемых шкафах (сейфах). При этом создаются надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить носители с персональными данными из служебных помещений без согласования с уполномоченным лицом.

После окончания работы сотрудники запирают полученные носители персональных данных в личный сейф, в случае его отсутствия сдают уполномоченному лицу.

Проверка наличия учитываемых носителей персональных данных проводится один раз в год комиссией или лицами, ответственными за обеспечение безопасности персональных данных.В ходе проверки

определяется перечень носителей персональных данных, которые (или информация на которых) подлежат уничтожению.

Уничтожение носителей персональных данных (или информации на них), утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных журналах об этом делается отметка со ссылкой на соответствующий акт.

6.8. Физические меры обеспечения информационной безопасности

Меры физической защиты предназначены для предотвращения несанкционированного физического доступа, повреждения и воздействия на помещения и информацию.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.8.1. Охраняемые зоны

Средства обработки персональных данных или важной служебной информации размещаются в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны физически защищаются от неавторизованного доступа, повреждения и воздействия. Уровень защищенности определяется соразмерно с идентифицированными рисками.

Для защиты зон, где осуществляется обработка, включая хранение, персональных данных и размещены средства обработки персональных данных, используются периметры охраняемых зон (периметры безопасности). Периметр безопасности - это граница, создающая барьер, например, проходная, оборудованная средствами контроля входа по идентификационным карточкам или сотрудник на стойке регистрации, вахтер.

Периметр безопасности четко определяется. Помещения, в которых осуществляется обработка, включая хранение, персональных данных, размещено оборудование, используемое при обработке персональных данных, устанавливаются и отражаются в частной модели угроз.

Помещения, в которых размещается оборудование, предназначенное для обработки информационных ресурсов, хранятся машиночитаемые носители и документы, содержащие конфиденциальную информацию, расположены рабочие места специалистов, осуществляющих обработку персональных данных, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, обеспечивать сохранность оборудования, машиночитаемых носителей информации и документов и защиту конфиденциальной информации от несанкционированного доступа.

Для этого входные двери этих помещений оборудуются надежными замками. Окна помещений, расположенных на первых или последних этажах

зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, защищаются металлическими решетками.

Определяются места регистрации и нахождения посетителей.

Контроль доступа в охраняемые зоны

Зоны информационной безопасности защищаются с помощью соответствующих мер контроля входа для обеспечения уверенности в том, что доступ позволен только авторизованному персоналу.

Права доступа сотрудников в зоны информационной безопасности (помещения, в которых осуществляется обработка персональных данных) определяются в соответствии с должностными обязанностями, регулярно анализируются и пересматриваются.

Посетители зон безопасности в обязательном порядке сопровождаются сотрудниками, имеющими право доступа в охраняемые зоны. Нахождение посторонних лиц и лиц, не имеющих права доступа к персональным данным, в помещениях охраняемой зоны допускается только в присутствии работников, ответственных за расположенные в них рабочие места.

Безопасность зданий, производственных помещений и оборудования

Зона информационной безопасности защищается путем закрытия на замок самого офиса или нескольких помещений внутри физического периметра безопасности, которые могут быть заперты и иметь запираемые файл-кабинеты или сейфы.

При этом предусматриваются следующие меры:

– основное оборудование, включая серверы, располагаются в местах с ограничением доступа посторонних лиц;

– подразделения поддержки и оборудование, например, фотокопировальные устройства и факсы, располагаются соответствующим образом в пределах зоны безопасности во избежание доступа, который мог бы скомпрометировать информацию;

– двери и окна запираются, когда в помещениях нет сотрудников, предусматривается внешняя защита окон – особенно низко расположенных;

– внедрение соответствующих систем обнаружения вторжений для внешних дверей и доступных для этого окон, которые подлежат регулярному тестированию. Аналогично оборудуются другие помещения, в которых расположены средства коммуникаций;

– справочники и внутренние телефонные книги, идентифицирующие местоположения средств обработки персональных данных и другой важной информации, не должны быть доступны посторонним лицам;

– обеспечивается надежное хранение опасных или горючих материалов на достаточном расстоянии от зоны информационной безопасности. Не допускается хранение больших запасов бумаги для печатающих устройств в зоне безопасности без соответствующих мер пожарной безопасности;

– резервное оборудование и носители данных располагаются на безопасном расстоянии во избежание повреждения от последствий стихийного бедствия в основном здании.

Выполнение работ в охраняемых зонах

В целях обеспечения защиты зон информационной безопасности выполняются следующие мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне безопасности:

– о существовании зоны информационной безопасности и проводимых в ней работах осведомляются только лица, которым это необходимо в силу производственной необходимости;

– из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах не допускаются случаи работы без надлежащего контроля со стороны уполномоченного персонала;

– персоналу третьих сторон ограниченный авторизованный и контролируемый доступ в зоны безопасности или к средствам обработки информации предоставляется только на время такой необходимости (например, для проведения регламентных (наладочных), ремонтных и других работ). Между зонами с различными уровнями безопасности внутри периметра безопасности могут организовываться дополнительные барьеры и периметры ограничения физического доступа;

– использование фото, видео, аудио или другого записывающего оборудования допускается только при получении специального разрешения руководителя оператора.

6.8.2. Безопасность оборудования

Основная цель мероприятий по обеспечению безопасности оборудования – предотвращение потерь, повреждений или компрометации информационных ресурсов и нарушения непрерывности деятельности оператора.

Оборудование подлежит защите от угроз его безопасности и воздействий окружающей среды с целью уменьшения риска неавторизованного доступа к данным и защиты их от потери или повреждения. При этом принимаются во внимание особенности, связанные с расположением оборудования и возможным его перемещением. При необходимости организуются специальные мероприятия защиты от опасных

воздействий среды или неавторизованного доступа через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

Расположение и защита оборудования

Оборудование располагается и защищается так, чтобы уменьшить риски от воздействий окружающей среды и возможности неавторизованного доступа. Для этого выполняются следующие правила:

а) оборудование размещается таким образом, чтобы свести к минимуму излишний доступ в места его расположения;

б) средства обработки и хранения конфиденциальной информации размещаются так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием;

в) отдельные элементы оборудования, требующие специальной защиты, изолируются, чтобы повысить общий уровень необходимой защиты;

г) меры по управлению информационной безопасностью должны сводить к минимуму риск потенциальных угроз, включая: воровство, пожар, взрыв, задымление, затопление (или перебои в подаче воды), пыль, вибрацию, химические эффекты, помехи в электроснабжении, электромагнитное излучение.

д) при необходимости оператором определяется порядок приема пищи, напитков вблизи средств обработки информации;

е) проводится мониторинг состояния окружающей среды в целях выявления условий, которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;

ж) разрабатываются меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице.

Подача электропитания

Оборудование подлежит защите от перебоев в подаче электроэнергии и других сбоев, связанных с электричеством. Необходимо обеспечить надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Варианты достижения непрерывности подачи электропитания включают:

- наличие нескольких источников электропитания, чтобы избежать последствий при нарушении его подачи от единственного источника;
- устройства бесперебойного электропитания (UPS);
- резервный генератор.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, с помощью которых осуществляется обработка, включая хранение, персональных данных, подключение оборудования должно осуществляться через UPS. В целях обеспечения надежности оборудование UPS следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.

Кроме того, аварийные выключатели электропитания располагаются около запасных выходов помещений, где расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

Безопасность кабельной сети

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или осуществляются другие информационные услуги,

защищаются от перехвата информации или повреждения. С этой целью рассматриваются, по возможности, следующие мероприятия:

а) силовые и телекоммуникационные линии, связывающие средства обработки информации, прокладываются подземными или обладают адекватной альтернативной защитой;

б) сетевой кабель защищается от неавторизованных подключений или повреждения, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков;

в) силовые кабели отделяются от коммуникационных, чтобы исключить помехи.

Техническое обслуживание оборудования

В организации проводится надлежащее техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и целостности. В этих целях применяются следующие мероприятия:

- оборудование обслуживается в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;
- техническое обслуживание и ремонт оборудования проводятся авторизованным персоналом;
- организуется хранение записей обо всех случаях предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;
- техническое обслуживание оборудования выполняется под контролем;
- принимаются соответствующие меры безопасности при отправке оборудования для технического обслуживания за пределы организации. Обязательным условием является удаление всех персональных данных и

иной конфиденциальной информации с носителей данных (встроенные жесткие диски).

Обеспечение безопасности оборудования, используемого вне помещений оператора

Независимо от принадлежности оборудования, его использование для обработки информации вне помещения оператора допускается только с разрешения руководства. Уровень информационной безопасности при этом должен быть эквивалентен уровню безопасности в отношении оборудования, используемого с аналогичной целью в помещениях оператора, а также с учетом рисков работы на стороне. Оборудование по обработке информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, а также бумагу или иные материальные ценности, которые используются для работы на дому или транспортируются за пределы рабочих помещений. В этих условиях необходимо применять следующие мероприятия по управлению информационной безопасностью:

– оборудование и носители информации, взятые из помещений оператора, не следует оставлять без присмотра в общедоступных местах. При перемещении компьютеры следует перевозить как ручную кладь и, по возможности, не афишировать ее содержимое;

– необходимо соблюдать инструкции изготовителей по защите оборудования, например, от воздействия сильных электромагнитных полей;

– при работе дома следует применять подходящие мероприятия по управлению информационной безопасностью с учетом оценки рисков, например, использовать запираемые файл-кабинеты, соблюдать политику «чистого стола» и контролировать возможность доступа к компьютерам.

Безопасная утилизация (списание) или повторное использование оборудования

Конфиденциальная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Носители данных, содержащие конфиденциальную информацию, кроме стандартных функций удаления подлежат физическому разрушению или перезаписыванию безопасным образом. Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), проверяются на предмет удаления всех защищаемых данных и лицензионного программного обеспечения.

7. Обеспечение безопасности персональных данных при обработке без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.

Документы, их копии, содержащие персональные данные получателей мер социальной поддержки, социального обслуживания, брошюруются в отдельные личные дела граждан. В случаях, предусмотренных законодательством, предоставления мер социальной поддержки в целом на

семью или отдельных ее членов персональные данные членов семьи подшиваются в личное дело на семью.

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

Личные дела граждан и/или семей хранятся обособленно от мест хранения материальных носителей с иной информацией.

Обеспечивается раздельное хранение материальных носителей с персональными данными (личных дел, других материальных носителей, содержащих персональные данные), обработка которых осуществляется в различных целях.

При хранении личных дел граждан и/или семей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Список лиц, имеющих доступ в помещения, в которых хранятся личные дела граждан и/или семей, утверждается приказом руководителя оператора.

В каждое личное дело получателя мер социальной поддержки, социального обслуживания приобщается заявление гражданина или его законного представителя. Заявление содержит следующие сведения:

– фамилию, имя, отчество гражданина (субъекта персональных данных);

– адрес проживания;

– серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование оператора, в адрес которого составлено заявление;

– цель обработки персональных данных (название меры социальной поддержки, вида социального обслуживания);

– срок обработки персональных данных (срок назначения меры социальной поддержки, установления вида социального обслуживания).

Заявление обязательно содержит поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных.

Личные дела граждан, семей, по которым истекли сроки обработки персональных данных (истекли сроки предоставления социальной поддержки, социального обслуживания), хранятся отдельно от личных дел с действующими сроками обработки персональных данных.

Сроки хранения личных дел граждан, семей, по которым истекли сроки обработки персональных данных, определяются в соответствии с «Перечнем типовых управленческих документов, образующихся в деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», утвержденным приказом Министерства культуры РФ от 25.08.2010 №558.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для учета обращений граждан, регистрации приема и/или выдачи документов, или в иных аналогичных целях, соблюдаются следующие условия:

– необходимость ведения журнала (реестра, книга), состав информации, запрашиваемой у субъектов персональных данных, предусмотрены нормативным правовым актом, регулирующим порядок предоставления мер социальной поддержки, социального обслуживания;

– список сотрудников, имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), утвержден приказом руководителя оператора;

– копирование содержащейся в журналах (реестрах, книгах) информации не допускается.

8. Обеспечение безопасности персональных данных при обработке в информационных системах персональных данных

Обработка персональных данных в информационных системах представляет собой обработку персональных данных, содержащихся в базах данных, с использованием информационных технологий и технических средств.

Основными элементами информационных систем персональных данных являются:

– персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в информационных системах персональных данных;

– информационные технологии, применяемые при обработке персональных данных;

– технические средства, осуществляющие обработку персональных данных;

– программные средства (операционные системы, системы управления базами данных и т.п.);

– средства защиты информации;

– вспомогательные технические средства и системы – технические средства и системы, их коммуникации, не предназначенные для обработки персональных данных, но размещенные в помещениях, в которых расположены информационные системы персональных данных, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации,

средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофиксации).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

При обработке персональных данных в информационной системе обеспечивается:

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

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

8.1. Методы и способы защиты информации от несанкционированного доступа

Методами и способами защиты информации от несанкционированного доступа являются:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

– организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

8.2. Технические меры обеспечения информационной безопасности

С учетом всех требований и принципов обеспечения безопасности персональных данных в информационных системах в состав системы защиты включаются следующие средства:

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем персональных данных;

– средства разграничения доступа зарегистрированных пользователей к ресурсам информационных систем персональных данных;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности.

Успешное применение технических средств защиты обеспечивается организационными (административными) мерами и используемыми физическими средствами защиты, направленными на выполнение следующих требований:

– обеспечение физической целостности всех компонентов информационных систем персональных данных;

– каждый сотрудник – пользователь информационной системы персональных данных или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– разработка и отладка программ осуществляется за пределами информационной системы персональных данных, на испытательных стендах;

– все изменения конфигурации технических и программных средств информационных систем персональных данных производятся строго установленным порядком (регистрируются и контролируются) только на основании указаний уполномоченного лица (структурного подразделения);

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

– осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Основные мероприятия по техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, представлены по следующим направлениям:

По антивирусной защите:

Предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок путем:

– непрерывного антивирусного мониторинга;

– проведения еженедельной проверки информационных ресурсов;

– ежедневного анализа событий фиксируемых журналом регистрации подсистемы антивирусной защиты;

– поддержания в актуальном состоянии базы вредоносных программ (программ-вирусов) и программных закладок.

По управлению доступом:

Идентификация и проверка подлинности пользователя осуществляется при входе в информационную систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

По регистрации и учету:

Регистрация входа (выхода) пользователя в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа.

По обеспечению целостности:

– обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

– физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

– периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

– контроль наличия средств восстановления системы защиты персональных данных, ведение двух копий программных компонентов средств защиты информации, периодическое обновление и контроль работоспособности копий системы защиты персональных данных.

По защите межсетевого взаимодействия:

– фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

– регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

– контроль целостности своей программной и информационной части;

– фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

– регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

– фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

– фильтрация с учетом любых значимых полей сетевых пакетов;

– регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

– регистрация запуска программ и процессов (заданий, задач).

По защите информации при подключении к сети Интернет:

– централизованное управление системой защиты персональных данных информационной системы;

– использование средств антивирусной защиты;

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование считывателей для надежной идентификациии аутентификации пользователей;

– фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);

– периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;

– активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

– анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

По защите информации при удаленном доступе и передаче по внешним каналам связи:

Защита информации при ее передаче по внешним каналам связи с использованием криптосредств по уровню КС1 (при установке на рабочие станции), КС2 (при организации защищенных каналов связи между взаимодействующими сетями (сегментами сетей)).

По управлению:

– централизованное управление системой защиты персональных данных информационной системы;

– управление доступом к защищаемым информационным системам персональных данных.

8.3. Перечень информационных систем

Обработка персональных данных осуществляется в следующих информационных системах органов социальной защиты населения Воронежской области:

– Государственная информационная система «Единая информационная система персонифицированного учета граждан в органах социальной защиты населения Воронежской области»;

– автоматизированные информационные системы кадрового учета;

– автоматизированные информационные системы бухгалтерского учета.

8.4. Классификация пользователей информационных систем персональных данных

Пользователем информационной системы является лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования. Пользователем информационных систем органов социальной защиты населения Воронежской области является любой работник, имеющий доступ к информационной системе и ее ресурсам (аппаратным средствам, программному обеспечению, данным, средствам защиты) в соответствии с установленным порядком, в соответствии с его должностными обязанностями.

Пользователи имеют различные права по доступу к защищаемым информационным ресурсам, размещенным на носителях различного уровня конфиденциальности.

Пользователи информационных систем персональных данных делятся на четыре основные категории:

1) Администратор информационной системы. Работникиорганов социальной защиты населения Воронежской области, в должностные обязанности которыхвходит настройка, внедрение и сопровождение системы. Администратор информационной системы обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении информационной системы;

– обладает полной информацией о технических средствах и конфигурации информационной системы;

– имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;

– обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

2) Администратор безопасности. Работники органов социальной защиты населения Воронежской области, в должностные обязанности которых входит обеспечение безопасности персональных данных. Администратор безопасности обладает следующим уровнем доступа:

– обладает полной информацией об используемых технических и программных средствах защиты информации;

– имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных.

3) Программист - разработчик информационной системы. Работники Департамента или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик информационной системы обладает следующим уровнем доступа:

– владеет информацией об алгоритмах и программах обработки информации в информационной системе;

– располагает информацией о топологии информационной системы и технических средствах обработки и защиты персональных данных, обрабатываемых в информационной системе.

4) Пользователь информационной системы. Работники органов социальной защиты населения Воронежской области, участвующие в процессе эксплуатации информационной системы. Пользователь информационной системы обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству персональных данных;

– располагает конфиденциальными данными, к которым имеет доступ.

Для каждого пользователя информационной системы персональных данных документально определены его категория, полномочия по доступу к защищаемым ресурсам.

С этой целью для каждой информационной системы персональных данных осуществляется ведение разрешительной системы доступа: формирование и корректировка списка пользователей информационной системы, установление их полномочий по доступу к защищаемым ресурсам.

8.5. Учет лиц, допущенных к персональным данным, обрабатываемым в информационных системах

Допуск к персональным данным, обрабатываемым в информационной системе, лицам, доступ которым к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей, производится в соответствии с разрешительной системой доступа.

Разрешительная система доступа должна быть составлена на каждую информационную систему персональных данных и должна содержать перечень лиц, допущенных к обработке персональных данных в информационной системе, с указанием уровня прав доступа.

Ведение разрешительной системы доступа возлагается приказом руководителя оператора на лиц, ответственных за обеспечение безопасности персональных данных.

Основанием для обеспечения доступа к персональным данным, обрабатываемых в информационных системах, и включения работников в разрешительную систему доступа являются сведения, подаваемых руководителями структурных подразделений оператора и должностные инструкции (должностные регламенты) работников.

8.6. Резервирование информации

В целях обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, осуществляется резервирование (резервное копирование) персональных данных.

Резервирование проводится на различные носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий осуществляется в надежных сейфах (металлических шкафах), в месте, территориально удаленном от основного хранилища информации.

Доступ к резервным копиям строго регламентируется.

Правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных устанавливают должностные лица Департамента, ответственные за обеспечение безопасности персональных данных при обработке в информационных системах.

Контроль над процессом осуществления резервного копирования объектов защиты возлагается на должностных лиц, ответственных за обеспечение безопасности персональных данных при обработке в информационных системах.

8.7. Организация парольной защиты

В целях обеспечения защиты от несанкционированного доступа к персональным данным и регистрации действий пользователей с персональными данными в информационных системах персональных данных организуется система парольной защиты.

Для обеспечения доступа к информационным системам персональных данных всем пользователям устанавливаются личные пароли. Личные пароли

доступа к средствам информационных систем персональных данных должны выдаваться пользователям лицом, ответственным за обеспечение безопасности персональных данных.

Правила формирования пароля:

1. Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
2. Пароль должен состоять не менее чем из 6 символов.
3. В пароле должны присутствовать символы трех категорий:
   – прописные буквы английского алфавита от A до Z;
   – строчные буквы английского алфавита от a до z;
   – цифры (от 0 до 9).

Обязательным требованием организации парольной защиты является полная плановая смена паролей в информационных системах персональных данных не реже одного раза в 3 месяца.

Лица, допущенные к обработке персональных данных в информационных системах, обязаны соблюдать требования парольной политики.

9. Контроль состояния обеспечения безопасности персональных данных

Основными целями контроля состояния обеспечения безопасности персональных данных являются:

– установление степени соответствия принятых мер по обеспечению безопасности персональных данных требованиям законодательных и иных нормативных актов, норм, правил и инструкций по обеспечению безопасности персональных данных;

– выявление потенциальных каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее, выработка рекомендаций по их закрытию.

Основными задачами контроля являются:

– оценка эффективности проводимых мер по обеспечению безопасности персональных данных;

– анализ причин выявленных нарушений и недостатков в организации и обеспечении безопасности персональных данных, выработка рекомендаций по их устранению;

– оценка и анализ возможностей злоумышленника по добыванию персональных данных, выявление каналов утечки информации, каналов несанкционированного доступа к информации и специальных воздействий на нее, выработка рекомендаций по закрытию этих каналов.

Контроль заключается в проверке выполнения законодательства Российской Федерации по вопросам защиты персональных данных, а также в оценке обоснованности и эффективности принятых мер защиты.

Эффективной формой контроля за выполнением требований настоящей Политики является проведения самооценки в форме внутренней проверки обеспечения безопасности персональных данных в органах социальной защиты населения Воронежской области, проводимой в соответствии с планом мероприятий по обеспечению безопасности персональных данных, разработанным комиссией Департамента по обеспечению безопасности персональных данных.

1. Организационный контроль состояния обеспечения безопасности персональных данных в органах социальной защиты населения Воронежской области проводится в форме внутренних проверок обеспечения безопасности персональных данных, проводимых в соответствии с планом проведения внутренних проверок. Организационный контроль проводится совместно с сотрудниками структурных подразделений, ответственными за вопросы обеспечения безопасности информации своих подразделениях.

2. Технический контроль состояния обеспечения безопасности персональных данных проводится в целях контроля функционирования системы защиты персональных данных, контроля установленных правил

(политик) безопасности, конфигурационных настроек средств защиты информации, входящих в состав системы защиты персональных данных. Организация и проведение технического контроля состояния обеспечения безопасности персональных данных возлагается на лиц, ответственных за обеспечение безопасности персональных данных.

Лица, ответственные за обеспечение безопасности персональных данных, осуществляют контроль за администрированием информационных систем в части вопросов обеспечения безопасности информации и взаимодействуют с администраторами информационных систем.

К техническому контролю состояния обеспечения безопасности персональных данных могут привлекаться специализированные организации, имеющие оформленные в установленном порядке лицензии на осуществление деятельности по технической защите конфиденциальной информации, оказывающие на договорной основе услуги по контролю (аудиту) состояния обеспечения безопасности персональных данных.

Перечень лицензий, необходимых привлекаемой специализированной организации, для оказания услуг по контролю состояния обеспечения безопасности персональных данных, включая контроль технических средств защиты конфиденциальной информации и криптосредств:

а) лицензия ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с

использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). Указанная лицензия должна, в том числе содержать следующие виды работ (услуг):

– разработка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;

– ремонт шифровальных (криптографических) средств;

– ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем;

– ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– ремонт, сервисное обслуживание средств изготовления ключевых документов;

– работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся

для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– передача шифровальных (криптографических) средств;

– передача защищенных с использованием шифровальных (криптографических) средств информационных систем;

– передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– передача средств изготовления ключевых документов;

– предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;

– изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

б)лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации. Указанная лицензия должна, в том числе, содержать следующие виды работ (услуг):

– контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации, технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается, помещениях со средствами (системами), подлежащими защите;

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– проектирование объектов в защищенном исполнении: средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите;

− установка, монтаж, испытания, ремонт средств защиты информации: технических средств защиты информации; защищенных технических средств обработки информации; технических средств контроля эффективности мер защиты информации; программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля защищенности информации).

в) лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации. Указанная лицензия должна, в том числе, содержать следующие виды работ (услуг):разработка средств защиты конфиденциальной информации, в том числе: защищенных программных (программно-технических) средств обработки информации.

Непосредственный контроль за выполнением требований Политики при обработке персональных данных осуществляют лица, ответственные за обеспечение безопасности персональных данных в органах социальной защиты населения Воронежской области.

9.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в Департаменте и подведомственных учреждениях проводятся плановые и внеплановые проверки условий обработки персональных данных. Проверки осуществляются лицами, ответственными за организацию

обработки персональных данных, по поручению руководителя Департамента (директора подведомственного учреждения).

В проведении проверки не может участвовать сотрудник Департамента (подведомственного учреждения), прямо или косвенно заинтересованный в ее результатах.

Внеплановые проверки могут проводиться на основании поступившего письменного заявления субъекта персональных данных о нарушениях правил обработки персональных данных.Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента поступления соответствующего заявления.

При проведении проверки соответствия обработки персональных данных установленным требованиям на основании поступившего письменного заявления субъекта персональных данных о нарушениях правил обработки персональных данных должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

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

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

Лицо, ответственное за организацию обработки персональных данных в Департаменте (подведомственном учреждении), либо комиссия при проведении проверки условий обработки персональных данных имеет право:

- запрашивать у служащих соответствующих структурных подразделений Департамента (подведомственного учреждения), осуществляющих обработку персональных данных либо доступ к ним, информацию, необходимую для реализации полномочий;

- требовать от сотрудников соответствующих структурных подразделений Департамента (подведомственного учреждения), осуществляющих обработку персональных данных либо доступ к ним, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- вносить руководителю Департамента (директору подведомственного учреждения) предложения по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю Департамента (директору подведомственного учреждения)предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке, а также предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области персональных данных.

Лицо, ответственное за организацию обработки персональных данных в Департаменте (подведомственном учреждении), либо комиссия при проведении проверки условий обработки персональных данных должны обеспечивать конфиденциальность персональных данных, которые стали известны в ходе проведения мероприятий внутреннего контроля.

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

По существу поставленных в обращении (жалобе) вопросов комиссия в течение 5 рабочих дней со дня окончания проверки дает письменный ответ заявителю.

Плановые проверки (внутренний контроль) осуществляются на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

Контролируемые вопросы в ходе проведения плановых проверок (внутреннего контроля):

– наличие у работников допуска к обработке персональных данных;

– наличие согласий субъектов на обработку их персональных данных;

– соблюдение целей, состава и сроков обработки персональных данных;

– соблюдение правил по обезличиванию персональных данных;

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

– соответствие полномочий сотрудников разрешительной системе доступа к информационным ресурсам, программным и техническим средствам информационной системы персональных данных;

– соблюдение сотрудниками парольной политики;

– соблюдение сотрудниками антивирусной политики;

– соблюдение сотрудниками правил работы со съемными носителями персональных данных;

– соблюдение порядка резервирования баз данных и хранения резервных копий;

– соблюдение порядка работы со средствами защиты информации.

По результатам проверки составляется протокол, который утверждается руководителем Департамента (директором подведомственного учреждения) и хранится у ответственного за обеспечение безопасности персональных данных в течение трех лет. При выявлении в ходе проверки нарушений в протоколе указываются мероприятия по устранению нарушений и сроки исполнения.

О результатах проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за организацию обработки персональных данных, докладывает руководителю Департамента (директору подведомственного учреждения).

10. Реагирование на инциденты нарушения информационной безопасности и сбои

Реагирование на инциденты нарушения информационной безопасности и сбои направлено на сведение к минимуму ущерба от инцидентов, а также осуществление мониторинга случаев инцидентов.

Инцидент – любое непредвиденное или нежелательное событие, которое может нарушать деятельность или информационную безопасность.

К инцидентам информационной безопасности относятся:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических защитных мер;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Реагирование на инциденты нарушения информационной безопасности включает в себя:

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

– разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Все работники немедленно сообщают о любых наблюдаемых или предполагаемых инцидентах нарушения информационной безопасности своему непосредственному руководителю и лицу, ответственному за информационную безопасность.

10.1. Информирование об инцидентах нарушения информационной безопасности

Все работники незамедлительно информируют своего непосредственного руководителя и лицо, ответственное за информационную безопасность, об инцидентах нарушения информационной безопасности.

Руководитель оператора в течение трех рабочих дней информирует о выявленном или предполагаемом инциденте комиссию Департамента по обеспечению безопасности персональных данных. В случае выявления фактов распространения персональных данных или утраты материальных носителей персональных данных руководитель оператора назначает комиссию по проведению служебного расследования.

Комиссия Департамента по обеспечению безопасности персональных данных осуществляет мониторинг и анализ инцидентов в целях выявления существенных инцидентов нарушения информационной безопасности, новых

уязвимостей, проверки эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности.

10.2. Информирование о проблемах безопасности

Все работники, осуществляющие обработку персональных данных, обязаны обращать внимание и сообщать непосредственному руководителю и лицу, ответственному за информационную безопасность, о любых замеченных или предполагаемых недостатках и угрозах в области безопасности персональных данных, в том числе в информационных системах персональных данных или сервисах. При этом не допускается самостоятельный поиск работниками оператора подтверждения подозреваемому недостатку в системе безопасности. Это требование предъявляется в интересах самих работников, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы.

10.3. Информирование о сбоях программного обеспечения

Работники, осуществляющие обработку персональных данных с использованием средств вычислительной техники, как в информационных системах, так и вне информационных систем, обязаны соблюдать следующий порядок действий в случаях сбоев используемого программного обеспечения:

– симптомы проблемы (сбоя) и любые сообщения, появляющиеся на экране, фиксируются (распечатываются, переписываются, сохраняются в электронном виде);

– компьютер изолируется (отключается от локальной вычислительной сети оператора), работа на нем прекращается;

– не допускается перенос информации с помощью внешних носителей на другие компьютеры;

– о проблеме немедленно извещается непосредственный руководитель, при работе в информационных системах – администратор баз данных и лицо, ответственное за информационную безопасность.

Пользователям запрещается самостоятельно удалять подозрительное программное обеспечение. Ликвидация последствий сбоев осуществляется обученным персоналом, либо под руководством и в соответствии с указаниями специалистов соответствующих структурных подразделений Департамента.

10.4. Реагирование на факты разглашения персональных данных

По каждому факту разглашения персональных данных или утраты материальных носителей персональных данных руководитель оператора незамедлительно назначает комиссию для проведения проверки, в состав которой обязательно включается представитель Департамента.

По факту утечки сведений из информационных систем персональных данных в состав комиссии обязательно должен быть включен представитель Комиссии Департамента по обеспечению безопасности персональных данных.

В ходе проверки устанавливаются все обстоятельства происшествия и виновные в утрате (разглашении) сведений, а также причины и условия, способствовавшие этому, определяются меры по локализации нежелательных последствий разглашения конфиденциальной информации.

По результатам проверки руководитель оператора принимает меры по устранению причин и условий, способствующих инциденту, а также, в случае выявления виновных лиц, принимает решение о привлечении виновных к ответственности.

11. Ответственность за нарушение требований информационной безопасности

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Ответственность за обеспечение требований по защите персональных данных и иной конфиденциальной информации возлагается на руководителя оператора.

Персональная ответственность – одно из главных требований по организации и проведению работ по обеспечению безопасности персональных данных и обязательное условие обеспечения эффективности этих работ.

Работники органов социальной защиты населения Воронежской области, имеющие доступ к информационным системам персональных данных и/или документам, содержащим персональные данные либо иную конфиденциальную информацию, должны быть ознакомлены с обязанностями по обеспечению безопасности информации и ответственностью за их нарушение.

1. Ответственность за утрату документов или машиночитаемых носителей с конфиденциальной информацией или разглашение сведений, содержащихся в них, персонально несет работник, допустивший утрату, разглашение.

2. Ответственность за несанкционированный доступ к персональным данным и иной конфиденциальной информации, совершение нерегламентированных действий с персональными данными, повлекшими их уничтожение, распространение, изменение, несет лицо, совершившее эти действия.

3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

Приложение 1

Типовая форма
согласия субъекта на обработку его персональных данных в связи с поступлением на работу в _____
_____

(наименование органа социальной защиты населения)

Я,_____
(фамилия, имя, отчество)
_____
(адрес)
_____
(паспорт: серия, номер, дата выдачи, кем выдан)
_____

В соответствии со статьями 86, 88 Трудового кодекса Российской Федерации, статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие _____
(наименование учреждения)
(далее - оператор), находящемуся по адресу: _____ ,
(адрес учреждения)
на обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (УФНС, ПФР, ФСС и т.д.), обезличивание, блокирование, уничтожение) моих персональных данных, в составе:

- фамилия, имя, отчество;
- число, месяц, год рождения;
- место рождения;
- гражданство;
- образование;
- владение иностранными языками;
- судимость;
- допуск к государственной тайне;
- выполняемая работа с начала трудовой деятельности;
- награды и знаки отличия;
- близкие родственники (степень родства, ФИО, год, число, месяц и место рождения, место работы, домашний адрес);
- пребывание за границей;
- отношение к воинской обязанности, воинское звание;
- домашний адрес (адрес регистрации, фактического проживания);
- номер телефона;
- документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан);

- наличие заграничного паспорта (серия, номер, кем и когда выдан)
- номер страхового свидетельства обязательного пенсионного страхования;
- ИНН.

Обработка моих персональных данных может осуществляться с использованием средств автоматизации и без использования таковых исключительно в целях реализации трудовых отношений.

Согласие вступает в силу с момента его подписания.

Оператор может осуществлять обработку моих персональных данных в течение срока действия служебного контракта (трудового договора) и в течение 75 (семидесяти пяти) лет после его прекращения.

Я вправе отозвать свое согласие на обработку персональных данных посредством письменного заявления.

«___»_____20__ г. (подпись) расшифровка подписи

Приложение 2

Журнал регистрации обращений и запросов субъектов персональных данных или их представителей
в _____
(наименование органа социальной защиты населения)

Начат «___»_____20__г.

Окончен «___»_____20__г.

Прошито, пронумеровано и опечатано _____ листов

№ п/п	Сведения о запрашивающем лице (субъекте персональных данных)	Номер, дата документа, удостоверяющего личность	Цель обращения/запроса	Действия по результатам обращения/запроса	Подпись ответственного лица	Примечание

Приложение 3

ТИПОВАЯ ФОРМА ОБЯЗАТЕЛЬСТВА
о неразглашении персональных данных граждан

Я, _____,
(ФИО сотрудника)
исполняющий(ая) должностные обязанности _____

_____,
(наименование должности и отдела)
обязуюсь:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный порядок передачи третьим лицам сведений, составляющих персональные данные граждан, которые мне будут доверены или станут известны в связи с исполнением своих должностных обязанностей.

2. Выполнять относящиеся ко мне требования положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, приказов, распоряжений, инструкций и других нормативных актов по обеспечению безопасности персональных данных.

3. В случае моего увольнения, все носители, содержащие персональные данные граждан, которые находились в моем распоряжении в связи с исполнением мною должностных обязанностей, передать непосредственному начальнику или сотруднику, определенному непосредственным начальником.

4. Немедленно сообщать непосредственному начальнику об утрате или недостаче документов или иных носителей, содержащих персональные данные граждан, и о других фактах, которые могут привести к разглашению персональных данных граждан, а также о причинах и условиях возможной утечки персональных данных.

5. После прекращения права на допуск к конфиденциальным сведениям, в том числе расторжения служебного контракта (трудового договора),прекратить обработку персональных данных, не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Об ответственности за разглашение персональных данных граждан предупрежден(а).

_____ _____
(подпись) *(расшифровка подписи)*

«___» _____ 20__ г.

Приложение 4

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ

субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Я, _____,
(фамилия, имя, отчество субъекта персональных данных или его представителя)

проживающий(ая) по адресу: _____,

основной документ: _____ номер: _____ серия:_____, кем и когда выдан: _____,

в соответствии с частью 2 статьи 18 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" настоящим подтверждаю, что мне разъяснены юридические последствия отказа предоставить свои персональные данные департаменту социальной защиты Воронежской области (или *наименование подведомственного учреждения*).

"___" _____ 20__ года _____ _____
(дата) *(подпись)* *(фамилия, инициалы)*