УТВЕРЖДЕНА

Приказом от _____ № _____

Политика информационной безопасности при обработке персональных данных в казенном учреждении Воронежской области «Детский дом города Воронежа»

Оглавление

Введение

Настоящая политика информационной безопасности при обработке персональных данных в казенном учреждении Воронежской области «Детский дом города Воронежа», (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в концепции информационной безопасности при обработке персональных данных в казенном учреждении Воронежской области «Детский дом города Воронежа», основной целью Политики является обеспечение безопасности казенного учреждения Воронежской области «Детский дом города Воронежа» 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 органы социальной защиты населения Воронежской области.

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»;

– методических документов ФСБ России, ФСТЭК России, Роскомнадзора;

– иных нормативных правовых актов в сфере защиты информации.

3. Область применения

Настоящая Политика распространяется в казенном учреждении Воронежской области «Детский дом города Воронежа» (далее – учреждение).

Требования настоящей Политики носят обязательный характер для всех работников учреждения (штатных, временных 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 казенном учреждении Воронежской области «Детский дом города Воронежа» 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 казенном учреждении Воронежской области «Детский дом города Воронежа» в связи с реализацией трудовых отношений, а также в связи с оказанием социальных услуг;

– перечень должностей служащих казенного учреждения Воронежской области «Детский дом города Воронежа», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

– типовое обязательство 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 казенного учреждении Воронежской области «Детский дом города Воронежа»;

– 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 казенном учреждении Воронежской области «Детский дом города Воронежа» на законной и справедливой основе.

Казенное учреждение Воронежской области «Детский дом города Воронежа» устанавливают следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

– издание нормативных 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 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 (предоставление, доступ), 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, 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 казенном учреждении Воронежской области «Детский дом города Воронежа»

Обработка персональных данных в казенном учреждении Воронежской области «Детский дом города Воронежа» осуществляется в целях 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 законной и справедливой основе;
- ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускает объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- только тех, содержание и объём которых отвечают заявленным целям их обработки;
- которые не должны быть избыточными по отношению к заявленным целям их обработки;
- обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

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 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 кадрового, бухгалтерского, социального учета. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных полномочий.

5.4. Категории субъектов, персональные данные которых обрабатываются в казенном учреждении Воронежской области «Детский дом города Воронежа»

К категориям субъектов, персональные данные которых обрабатываются в казенном учреждении Воронежской области «Детский дом города Воронежа», относятся:

- работники казенного учреждения Воронежской области «Детский дом города Воронежа»;
- воспитанники казенного учреждения Воронежской области «Детский дом города Воронежа».

5.5. Сроки обработки и хранения персональных данных

Персональные данные, связанные с реализацией трудовых отношений, обрабатываются и хранятся в течение срока действия 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, 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 директором 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 в казенном учреждении Воронежской области «Детский дом города Воронежа», включаются в состав электронных архивов и хранятся согласно установленным законодательством срокам отдельно от баз данных информационных систем казенном учреждении Воронежской области «Детский дом города Воронежа».

5.7. 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.

5.8. 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.

Форма согласия на обработку персональных данных работников казенного учреждении Воронежской области «Детский дом города Воронежа» приведена в приложении 1 к настоящей Политике.

В случае отказа субъекта предоставить персональные данные, утвержденные локальными актами учреждения или согласие на их обработку оператор обязан разъяснить субъекту персональных данных юридические последствия такого отказа.

5.9. Право субъекта персональных данных на доступ к своим персональным данным

Субъект (его законный представитель) имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к субъекту, а также на ознакомление с такими персональными данными. Субъект вправе требовать от оператора уточнения своих персональных данных или

уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения о наличии персональных данных предоставляются субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

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

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

– подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

– способы обработки персональных данных, применяемые оператором;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

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

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

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:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- обеспечение своевременного обнаружения фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- обеспечение возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

6.1. Организационная структура управлением информационной безопасности

В целях эффективного управления системой защиты персональных данных в казенном учреждении Воронежской области «Детский дом города Воронежа», своевременного реагирования на изменения в информационной структуре, существенно влияющих на установленные уровни безопасности информации, в учреждении.

В целях реализации мероприятий по обеспечению безопасности персональных данных в учреждении назначаются ответственные лица.

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

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

1. В информационных системах, предназначенных для обработки персональных данных сотрудников учреждения в целях осуществления кадрового учета – инспектор по кадрам.
2. В информационных системах, предназначенных для обработки персональных данных учреждения в целях осуществления бухгалтерского учета – работники бухгалтерской службы.

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

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.

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.

При вступлении в должность нового сотрудника инспектор по кадрам, 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.

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

Решение об организации доступа к сети Интернет на конкретных компьютерах принимается директором учреждения 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 ПО 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 казенного учреждения Воронежской области «Детский дом города Воронежа».

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 казенного учреждения

Воронежской области «Детский дом города Воронежа» 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 казенном учреждении Воронежской области «Детский дом города Воронежа», 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 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.

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.

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.

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).

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;

– 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

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;

– 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;

– 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.

8.3. Перечень информационных систем

Обработка персональных данных осуществляется в следующих информационных системах учреждения:

– автоматизированные информационные системы кадрового учета;

– автоматизированные информационные системы бухгалтерского учета.

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.

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 оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических защитных мер;
- 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.

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

11. Ответственность за нарушение требований информационной безопасности

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о субъектах, 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 директора 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 учреждения, 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

К приказу от _____ № _____

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

_____
_____
Паспорт серия_____№ _____
выдан«____»_____ _____ г.
зарегистрированной(го) по адресу:_____
_____
_____

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим я, _____, представляю КУ ВО «Детский дом г. Воронежа» зарегистрированному по адресу: г. Воронеж, ул. Острогожская, 57 Работодателю (оператору), свои персональные данные в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов при содействии в трудоустройстве, обучении и продвижении по работе, обеспечения личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2), трудовой книжке и полученная в течение срока действия настоящего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, адреса фактического места проживания и регистрации по местожительству, почтовые и электронные адреса, номера телефонов, биометрические данные, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора.

Своей волей и в своих интересах выражаю согласие на осуществление Работодателем (оператором) любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных,

включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение; передачу Работодателем (оператором) по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам, включая банки, налоговые органы, в отделения пенсионного фонда, фонда социального страхования, фонда обязательного медицинского страхования, уполномоченным агентам и организациям; хранение моих персональных данных в течение 75 лет, содержащихся в документах, образующихся в деятельности Работодателя (оператора), согласно части 1 статьи 17 Закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», а также при осуществлении любых иных действий с моими персональными данными, указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

_____ «___» _____ 20____ г.

Приложение 2

К приказу от _____ № _____

Журнал регистрации обращений и запросов субъектов персональных данных или их представителей в КУ ВО «Детский дом г. Воронежа»

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

К приказу от _____ № _____

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
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.