Приложение № 1

УТВЕРЖДАЮ:
Директор бюджетного
учреждения Воронежской области
«Песковский центр реабилитации
и социализации»

_____ Н.А. Сочнова
Приказ от 29.12.2023 года № 150/ОД

ПОЛОЖЕНИЕ

Об обработке и защите персональных данных работников
бюджетного учреждения Воронежской области
«Песковский центр реабилитации и социализации»

Содержание

Термины и определения

В рамках настоящего Положения используются следующие термины, определения и понятия:

- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;
- **информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- **конфиденциальность персональных данных** - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным субъектов, требование не допускать их распространения без согласия субъекта или иного законного основания;
- **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- **обработка персональных данных безиспользования средств автоматизации (неавтоматизированная)** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектовперсональных данных, осуществляются при непосредственном участии человека;
- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами РФ не распространяется требование соблюдения конфиденциальности;
- **оператор** - государственный орган,муниципальный орган, юридическое или физическое лицо, организующиеи (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
- **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- **субъект персональных данных** - физическое лицо, чьи персональные данные подлежат обработке;
- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1 Общие положения

1.1. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в министерстве социальной защиты Воронежской области (далее - Положение) разработано в целях организации обработки персональных данных сотрудников и иных субъектов, персональные данные которых подлежат обработке в бюджетном учреждении Воронежской области «Песковский центр реабилитации и социализации», определения порядка получения, обработки, передачи персональных данных, установления прав, обязанностей и ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и общий порядок организации работ по обеспечению безопасности персональных данных.

1.2. Настоящее Положение разработано на основе «Концепции информационной безопасности при обработке персональных данных в органах социальной защиты населения Воронежской области», утверждаемой приказом Департамента, Политики информационной безопасности и в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях, Гражданского кодекса Российской Федерации, Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлений 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», от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказов Федеральной службы по техническому и экспортному контролю Российской Федерации от11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других нормативных правовых актов.

1.3 Целью организации обработки персональных данных и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах

бюджетного учреждения Воронежской области «Песковский центр реабилитации и социализации» (далее - Учреждение) является обеспечение конституционных прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Обработка персональных данных должна осуществляться на основе следующих принципов:

- обработка персональных данных должна осуществляться на законном основании;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- бюджетное учреждение Воронежской области «Песковский центр реабилитации и социализации» должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных 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;
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- соблюдения принципов и правил обработки персональных данных при поручении такой обработки другому лицу;
- соблюдение конфиденциальности персональных данных;

- соблюдением обязанностей, возлагаемых на бюджетное учреждение Воронежской области «Песковский центр реабилитации и социализации» персональных данных, действующим законодательством и иными нормативными актами по персональным данным;
- принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных;
- недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;
- документального оформления всех принятых решений по обработке персональных данных.

Требования настоящего Положения должны пересматриваться при появлении новых угроз безопасности персональных данных, при изменении организационной структуры системы защиты персональных данных Учреждения, в других случаях при необходимости внесения изменений в организацию и порядок проведения работ по защите информации.

2 Область применения

Требования настоящего Положения носят обязательный характер для всех сотрудников Учреждения, в целях выполнения должностных обязанностей имеющих доступ к персональным данным, а также для сотрудников Учреждения, на которых возложено решение задач обеспечения безопасности персональных данных. Работники Учреждения, участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

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

Обработка персональных данных в информационных системах Учреждения должна осуществляться на законной и справедливой основе.

Учреждение устанавливает следующие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

- издание нормативных правовых актов 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 работников Учреждения, 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, обеспечение обучения указанных работников;
- 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;

- 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.

4 Порядок обработки персональных данных в Учреждении

4.1 Определение способов обработки персональных данных в Учреждении

Обработка персональных данных подразделяется на:

- обработка персональных данных, осуществляемая в автоматизированном режиме (в информационных системах (ИС));

- обработка персональных данных, осуществляемая без использования средств автоматизации.

4.2 Обработка персональных данных в автоматизированном режиме

Обработка персональных данных в ИС с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

Не допускается обработка персональных данных в ИС с использованием средств автоматизации, если применяемые меры и средства обеспечения безопасности не соответствуют требованиям, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Обработка персональных данных с использованием средств автоматизации осуществляется в рамках ИС Учреждения и внешних информационных систем, предоставляемых сторонними организациями. Состав ИС Учреждения приведен ниже:

- Единая информационная система персонифицированного учёта граждан в органах социальной защиты Воронежской области.

- Информационная система «1С. Предприятие. Зарплата и кадры бюджетного учреждения, редакция 1.0».

- Программный комплекс СБиС+ электронная отчетность.

4.3 Обработка ПДн, осуществляемая без использования средств автоматизации

Сотрудники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Учреждения.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; имени (наименовании) и адресе Учреждения; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональных данных, которые будут совершаться в процессе их обработки; общее описание используемых Учреждением способов обработки персональных данных;

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

-типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

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 должен использоваться отдельный материальный носитель.

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

Порядок обработки персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации осуществляется в рамках осуществления кадровой и бухгалтерской работы с персоналом Учреждения, в том числе присвоения квалификационных категорий, подготовки и переподготовки, проведения конкурсов, конференций, обучающих семинаров, а также в рамках повышения качества оказываемых услуг (прием жалоб граждан на качество оказываемых услуг).

Обработка персональных данных без использования средств автоматизации, осуществляемая в рамках ведения кадровой деятельности Учреждения, осуществляется при заключении трудового договора с работником, заполнении им личной карточки формы Т-2, автобиографии и другой необходимой при приеме на работу документации:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка, за исключением случаев, когда работник принимается на работу впервые или на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу (военный билет);
- документы об образовании, о квалификации или наличии специальных знаний (диплом, свидетельство об аттестации и присвоении категории, документ об усовершенствовании или специализации);
- документы о присвоении ученой степени, ученого звания;
- документы, подтверждающие те или иные факты, касающиеся жизни сотрудника (например, свидетельство о заключении брака и расторжении брака, свидетельство о рождении ребенка);
- документы, подтверждающие наличие наград, присвоении званий и т.д.;
- свидетельство о постановке на учет в налоговом органе (при наличии);
- необходимые справки (например, справка о доходах по форме НДФЛ-2 с прежнего места работы).

4.4 Цели обработки персональных данных

Обработка персональных данных в Учреждении осуществляется в целях:

- выполнения полномочий по реализации на территории области государственной политики по социальной поддержке и социальному обслуживанию населения;
- организации кадрового и бухгалтерского учета сотрудников Учреждения.

4.5 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 полномочий Учреждения. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных полномочий.

Субъектами персональных данных, сведения о которых обрабатываются в информационных системах Учреждения, являются:

- работники - сотрудники Учреждения по трудовым договорам/служебным контрактам, физические лица, с которыми заключены договоры на оказание услуг, бывшие сотрудники, уволившиеся из Учреждения;
- соискатели - кандидаты для приема на работу в Учреждение;
- граждане, обратившиеся за получением государственных и иных услуг.

Для перечисленных субъектов персональных данных Учреждение выполняет функции оператора.

Оператор получает сведения о персональных данных субъекта из следующих источников:

- информация, представляемая гражданином при обращении за социальной поддержкой, социальным обслуживанием: паспорт или иной документ, удостоверяющий личность, удостоверение о праве на льготы, документы МСЭ, страховое свидетельство обязательного пенсионного страхования, справка о составе семьи, справка о доходах, другие документы, установленные порядком предоставления социальной поддержки, социального обслуживания;
- информация, представляемая работником при поступлении на работу в Учреждение: паспорт или иной документ, удостоверяющий личность, трудовая книжка, страховое свидетельство обязательного пенсионного страхования, документы воинского учета, документ об образовании, о квалификации или наличии специальных знаний, свидетельство о присвоении ИНН;
- анкетные сведения, заполняемые субъектом персональных данных при обращении

или при приеме на работу;

- иные документы и сведения, предоставляемые субъектом персональных данных;

сведения, полученные в рамках межведомственного информационного взаимодействия, в том числе через систему межведомственного электронного взаимодействия.

4.6 Условия и порядок обработки 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.

Обработка персональных данных осуществляется оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных федеральными законами.

Субъект персональных данных является собственником своих персональных данных и самостоятельно по своей воле принимает решение о передаче оператору своих персональных данных и дает согласие на их обработку, за исключением случаев, предусмотренных федеральным законодательством. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случае отказа предоставить ПДн оператор обязан разъяснить субъекту ПДн или его законному представителю юридические последствия отказа предоставления ПДн.

Получение, хранение, передача или любое другое использование персональных данных субъекта персональных данных осуществляется исключительно в целях реализации основных полномочий Учреждения, обеспечения соблюдения законов и иных нормативных правовых актов.

Получение персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения их из иных источников.

Если планируется получение персональных данных у третьей стороны, то субъект уведомляется об этом заранее и от него должно быть получено письменное согласие. Оператор сообщает субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

Обработку персональных данных в Учреждении осуществляют должностные лица, допущенные к данной обработке.

Состав должностных лиц, имеющих доступ к обработке персональных лиц, определяется на основе заявок руководителей структурных подразделений

Учреждения на предоставление прав (полномочий) доступа пользователя к персональным

данных.

Внутри Учреждения к разряду потребителей персональных данных, помимо руководителя и его заместителей, относятся сотрудники структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- сотрудники отдела бюджетного учета и сводной отчетности (ведущий консультант, старший инспектор);

- сотрудники отдела кадров (ведущий советник, консультант, старший инспектор);

- сотрудники отдела развития информационных ресурсов (заместитель начальника отдела, ведущий консультант); <

- сотрудники отдела предоставления гражданам субсидий и компенсаций на оплату жилищно-коммунальных услуг (начальник отдела, заместитель начальника отдела, ведущий консультант, консультант, старший инспектор);

- сотрудники отдела социальной поддержки федеральных, региональных льготников и отдельных категорий граждан (начальник отдела, заместитель начальника отдела, ведущий консультант, консультант, старший инспектор);

- сотрудники отдела организации стационарного обслуживания граждан пожилого возраста и инвалидов (заместитель начальника отдела, ведущий консультант, консультант, старший инспектор);

- сотрудники отдела организации комплексного социального обслуживания населения (начальник отдела, заместитель начальника отдела, ведущий консультант, консультант, старший инспектор);

- сотрудники отдела организации социального обслуживания семьи, женщин и детей (заместитель начальника отдела, ведущий консультант, консультант, старший инспектор);

- сотрудники отдела предоставления жилья отдельным категориям граждан (начальник отдела, заместитель начальника отдела, ведущий консультант);

- сотрудники отдела обеспечения граждан техническими средствами реабилитации и санаторно-курортным лечением (начальник отдела, заместитель начальника отдела, ведущий консультант, специалист);

- сотрудники контрольно-ревизионного отдела (ведущий консультант);

- сотрудники отдела организации делопроизводства и работы с обращениями граждан (ведущий консультант, старший инспектор).

Учреждение на основании договора может поручать обработку персональных данных третьим лицам. Передача документов (иных материальных носителей), содержащих персональные данные, третьим лицам осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг или соглашения об информационном взаимодействии;
- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных граждан;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные гражданина, ее перечень, цель использования, фамилию, имя, отчество и должность лица, которому поручается получить данную информацию.

Передача персональных данных третьим лицам осуществляется с составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные субъектов.

Не допускается получение и обработка персональных данных субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

Процедура оформления доступа к персональным данным субъекта предусматривает ознакомление с настоящим Положением, лиц, допущенных к обработке персональных данных, под роспись, а также истребование с лиц, допущенных к обработке персональных данных, письменного обязательства о соблюдении конфиденциальности персональных данных субъекта и соблюдении правил их обработки.

4.7 Правила рассмотрения запросов субъектов персональных данных или их представителей

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

Обращения субъектов персональных данных о соблюдении их законных прав регистрируются Учреждением - оператором в специальном журнале.

Сведения о наличии персональных данных при обращении субъекта персональных данных предоставляются субъекту персональных данных оператором в доступной форме, 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 содержит 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. Запрос может быть направлен в электронной форме и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных 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.

4.8 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 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.

4.9 Лицо, ответственное за организацию обработки персональных данных в Учреждении

Приказом Учреждения назначается лицо, ответственное за организацию обработки персональных данных в Учреждении (далее - Ответственное лицо).

Ответственное лицо получает указания непосредственно от руководителя Учреждения и

подотчетно ему.

Ответственное лицо обязано:

- осуществлять внутренний контроль за соблюдением в Учреждении законодательства Российской Федерации о персональных данных, в том числе за соблюдением правил обработки персональных данных;

- доводить до сведения сотрудников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите 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.

5 Общая характеристика информационных систем персональных данных

Обработка персональных граждан осуществляется в следующих информационных системах Учреждения:

В целях организации и управления деятельностью органов социальной защиты населения по реализации полномочий по предоставлению гражданам социальной поддержки:

Государственная информационная система «Единая информационная система персонифицированного учета граждан в органах учета граждан в органах социальной защиты населения Воронежской области» предназначена для автоматизации процессов принятия решений и предоставления мер социальной поддержки населению путем формирования и использования единой базы данных в масштабах Воронежской области, содержащей комплексную информацию о лицах, нуждающихся в социальном обеспечении/или социальном обслуживании.

Содержит следующие сведения субъекта персональных данных:

- фамилия, имя, отчество, дата рождения субъекта персональных данных;
- данные документа, удостоверяющего личность субъекта персональных данных;
- номер страхового свидетельства обязательного пенсионного страхования;
- адрес места жительства субъекта персональных данных.
- данные документа (удостоверения, справки и др.), подтверждающего право на меры социальной поддержки;
- при наличии, сведения об установлении инвалидности;
- награды и знаки отличия;
- сведения о составе семьи;
- сведения об жилищных условиях;

- сведения о доходах;
- сведения о предоставленных мерах социальной поддержки.

В целях бухгалтерского учета (начисления заработной платы) используется программный продукт ««1С. Предприятие. Зарплата и кадры бюджетного учреждения, редакция 1.0», включающий следующие сведения:

- фамилия, имя, отчество, дата рождения субъекта персональных данных;
- данные документа, удостоверяющего личность субъекта персональных данных;
- адрес места жительства субъекта персональных данных;
- должность субъекта персональных данных;
- номер приказа и дату приема на работу (увольнения) субъекта персональных данных;
- ИНН субъекта персональных данных;
- номер страхового свидетельства обязательного пенсионного страхования субъекта персональных данных;
- сведения о доходах.

В целях кадрового учета используется программный продукт «1С. Предприятие. Зарплата и кадры бюджетного учреждения, редакция 1.0», включающий следующие сведения:

- фамилия, имя, отчество субъекта персональных данных;
- число, месяц, год и место рождения;
- гражданство;
- образование;
- владение иностранными языками;
- судимость;
- 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)
- ИНН субъекта персональных данных;

- номер страхового свидетельства обязательного пенсионного страхования субъекта персональных данных;
- сведения о доходах.

6 Правила работы с обезличенными персональными данными

Обезличивание персональных данных в Учреждении может проводиться 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.

Отдел развития информационных ресурсов Учреждения готовит предложения по обезличиванию персональных данных, обоснование такой необходимости и способы обезличивания.

Список лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом Учреждения.

Контроль за соблюдением проводимых мероприятий по обезличиванию персональных данных осуществляется в рамках внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных.

7 Обеспечение безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных являются составной частью управленческой и производственной деятельности Учреждения и осуществляются во взаимосвязи с другими мерами по обеспечению защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

Информационная безопасность - механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации авторизованных пользователей по мере необходимости.

Организация и проведение работ по обеспечению безопасности персональных данных в Учреждения осуществляются в соответствии со следующими принципами:

- законности осуществляемых в Учреждении целей, способов обработки персональных данных и мероприятий по обеспечению безопасности персональных данных;
- обеспечения баланса интересов государства, Учреждения, работников и иных субъектов, персональные данные которых подлежат обработке в Учреждении;
- обеспечения соответствия осуществляемых в Учреждении мероприятий по обеспечению безопасности персональных данных требованиям правовых, нормативных и методических документов федеральных органов исполнительной власти, уполномоченных в области защиты персональных данных;
- обеспечения соответствия осуществляемых в Учреждении мероприятий по обеспечению безопасности персональных данных составу и уровню опасности угроз безопасности персональных данных;
- комплексности проводимых мероприятий по обеспечению безопасности персональных данных;
- непрерывности и преемственности мероприятий по обеспечению безопасности персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных (достаточности персональных данных для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных).

Под организацией обеспечения безопасности персональных данных при их обработке в информационных системах понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от возможной реализации угроз безопасности персональных данных в информационных системах, и осуществляемых на всех стадиях жизненного цикла информационных систем персональных данных в целях:

- предотвращения возможных (потенциальных) угроз безопасности;
- нейтрализации и/или парирования реализуемых угроз безопасности;
- ликвидации последствий реализации угроз безопасности и восстановления нормального функционирования информационных систем персональных данных.

Система защиты персональных данных, в общем случае, представляет собой совокупность

организационных мер и технических средств защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемых в информационных системах персональных данных информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности персональных данных. Структура, состав и основные функции системы защиты персональных данных определяются в соответствии с частными моделями угроз безопасности персональных данных и классами информационных систем персональных данных.

Основные меры обеспечения безопасности персональных данных определены в Политике информационной безопасности.

8 Структура организационной системы обеспечения безопасности персональных данных

Управление и координация деятельности Учреждения по обеспечению безопасности персональных данных осуществляются комиссией Учреждения по обеспечению безопасности персональных данных (далее - комиссия Учреждения).

Организация работ по обеспечению безопасности персональных данных и поддержанию достигнутого уровня защиты персональных данных на этапах эксплуатации информационных систем персональных данных в Учреждении возложены на отдел развития информационных ресурсов Учреждения.

В целях обеспечения безопасности персональных данных отдел развития информационных ресурсов Учреждения взаимодействует со всеми структурными подразделениями Учреждения, сотрудники которых имеют доступ к информационным системам персональных данных.

В зависимости от задач и целей создания информационных систем персональных данных, а также обрабатываемых в них персональных данных ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах назначаются сотрудники Учреждения.

Ответственность за организацию и выполнение правил обеспечения безопасности персональных данных в отделах Учреждения возложена на начальников отделов Учреждения.

Комиссия Учреждения:

Осуществляет руководство деятельностью по разработке и актуализации документов Учреждения по обеспечению безопасности персональных данных, в том числе:

- приказов Учреждения по вопросам безопасности персональных данных;
- перечня сведений конфиденциального характера;
- положений, руководств, регламентов и инструкций по вопросам организации и

контроля обеспечения информационной безопасности.

Осуществляет контроль выполнения требований документов, регламентирующих деятельность по обеспечению информационной безопасности работниками Учреждения.

Отдел развития информационных ресурсов Учреждения:

Отвечает за ведение и актуализацию документов Учреждения по обеспечению безопасности персональных данных, в том числе:

- списков сотрудников, допущенных к обработке персональных данных (по подразделениям Учреждения, по информационным системам);
- актов классификации информационных систем персональных данных;
- моделей (частных моделей) угроз безопасности информационных систем персональных данных.

Руководит и контролирует работу лиц, ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах, в части реализации правил (политик) безопасности (разрешительная система доступа), настроек средств защиты информации, состава пользователей информационных систем.

Отвечает за ведение и актуализацию эксплуатационной документации Учреждения по обеспечению безопасности персональных данных, в том числе:

- журналов учета выданных паролей;
- журналов учета внешних носителей персональных данных;
- документации на средства защиты информации, включая лицензии, сертификаты.

Начальники отделов Учреждения, ответственные за вопросы обеспечения информационной безопасности в своих подразделениях:

- организуют контроль выполнения мероприятий по защите персональных данных в подразделениях;
- отвечают за ведение и актуализацию списка сотрудников, допущенных к обработке персональных данных (по информационным системам);
- отвечают за своевременную подачу заявок на допуск сотрудников к обработке персональных данных в информационных системах Учреждения;
- отвечают за своевременное предоставление информации об исключении из списка лиц, допущенных к обработке персональных данных в информационных системах, сотрудников отделов (в связи с увольнением, изменением должностных обязанностей, переводом на другую работу (должность, отдел) и т.д.).

Лица, ответственные за обеспечение безопасности персональных данных при их обработке

в информационных системах:

- осуществляют контроль за администрированием информационных систем в части вопросов обеспечения информационной безопасности;

- взаимодействуют с администраторами информационных систем.

Администраторы информационных систем:

- осуществляют администрирование информационных систем персональных данных Учреждения.

Пользователи информационных систем персональных данных:

- осуществляют обработку персональных данных в информационных системах персональных данных Учреждения согласно установленным для них правам доступа и полномочиям;

- отвечают за выполнение правил обработки персональных данных и правил доступа к информационным ресурсам информационных систем персональных данных, установленными положениями, регламентами и инструкциями Учреждения;

- отвечают за целостность и сохранность установленных на их автоматизированных рабочих местах средств защиты информации;

- отвечают за правильное использование внешних носителей персональных данных, их своевременный учет в журналах учета внешних носителей персональных данных.

9 Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных

Помещения, в которых размещается оборудование, предназначенное для обработки персональных данных в информационных системах, 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, защиту конфиденциальной информации от несанкционированного доступа.

Для этого входные двери этих помещений оборудуются прочными, оборудованными надежными замками. Окна помещений, расположенных на первых этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, защищаются металлическими решетками.

В помещениях, где размещены технические средства, участвующие в обработке персональных данных, а также хранятся носители персональных данных (далее - Помещения), право самостоятельного доступа имеют только сотрудники Учреждения, рабочие места которых размещены в соответствующем Помещении.

Нахождение посторонних лиц и лиц, не имеющих права доступа к персональным данным, в этих помещениях допускается только в присутствии работников, ответственных за расположенные в них рабочие места. При этом исключается возможность доступа посторонних лиц к обрабатываемым персональным данным через выводимую на экран монитора и принтер информацию, а также к носителям персональных данных.

Средства вычислительной техники, с помощью которых осуществляется обработка персональных данных и другой конфиденциальной информации, располагаются таким образом, чтобы был исключен несанкционированный просмотр информации, выводимой на экраны мониторов и на другие средства отображения информации.

В рабочее время, в случае ухода всех сотрудников, имеющих право самостоятельного доступа, из Помещения, а также в нерабочее время дверь в Помещение закрывается на ключ.

Уборка Помещения проводится только в присутствии сотрудника, имеющего право самостоятельного доступа в Помещение.

Техническое обслуживание средств вычислительной техники, коммуникационного оборудования, входящих в состав объекта информатизации, осуществляется только персоналом, допущенным к техническому обслуживанию под наблюдением сотрудника, ответственного за автоматизированное рабочее место. При проведении данных работ обработка конфиденциальной информации запрещена.

На время проведения ремонта Помещения все технические средства, участвующие в обработке персональных данных, а также носители персональных данных переносятся в другое Помещение, используемое для обработки персональных данных.

Для проведения регламентных (наладочных), ремонтных и других работ во время обработки конфиденциальной информации посторонние лица допускаются в эти помещения только в экстренных случаях по согласованию с должностным лицом, ответственным за обеспечение информационной безопасности, и в присутствии лиц, ответственных за обработку персональных данных, при условии исключения несанкционированного доступа к персональным данным и иной конфиденциальной информации и контроля за порядком осуществления проводимых работ.

Ремонт (вне помещений Учреждения), списание, утилизация (выбытие), реализация и другие действия с оборудованием, на котором обрабатывались или хранились информационные системы персональных данных, осуществляется только при условии, если информация, находящаяся на носителях информации этого оборудования, надежно удалена (стерта) без возможности ее восстановления и последующего прочтения, о чем составляется соответствующий

Контроль за соблюдением порядка доступа сотрудников в Помещения осуществляют начальники отделов Учреждения.

10 Организация доступа к персональным данным

Организация доступа к персональным данным реализуется оператором с соблюдением принципов конфиденциальности, доступности и целостности таких данных.

Обеспечение конфиденциальности персональных данных не требуется:

- в отношении общедоступных персональных данных;
- в случае обезличивания персональных данных.

Доступ к персональным данным субъекта имеют сотрудники Учреждения в соответствии с занимаемой должностью, правами и полномочиями, которым эти данные необходимы для выполнения должностных обязанностей.

Сотрудники Учреждения, которым персональные данные необходимы для выполнения должностных обязанностей, подписывают обязательство о неразглашении персональных данных субъектов. Форма обязательства приведена в приложении 4 к настоящему Положению.

Правила и порядок оформления доступа сотрудников Учреждения к персональным данным, а также порядок разграничения доступа к ним определяются положением о разрешительной системе доступа Учреждения.

Доступ сторонних организаций к персональным данным осуществляется в соответствии с действующим законодательством, а также в рамках реализации договорных отношений или по письменным запросам, по решению руководителя Учреждения.

Доступ сотрудников Учреждения к персональным данным может быть приостановлен по решению должностных лиц, ответственных за обеспечение безопасности персональных данных, в следующих случаях:

- увольнение работника;
- выявление нарушений работником правил обработки и защиты персональных данных, установленных федеральным законодательством, локальными нормативными правовыми актами Учреждения, настоящим Положением;
- изменение должностных обязанностей, перевода на другую работу.

11 Организационные меры обеспечения безопасности персональных данных, связанные с персоналом

Все сотрудники, имеющие доступ к персональным данным, обязаны четко 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 федеральных органов исполнительной власти, органов исполнительной власти

Воронежской области, настоящим документом.

Все сотрудники, осуществляющие обработку персональных данных, подписывают обязательство о неразглашении персональных данных граждан.

При вступлении в должность нового сотрудника начальник отдела, в который он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, настоящим документом, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования персональных данных.

12 Обязанности лиц, допущенных к обработке персональных данных в информационных системах

Лица, допущенные к обработке персональных данных, 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.;
- не оставлять незапертыми помещения, в которых расположены рабочие места работников, имеющих доступ к персональным данным, на время отсутствия работников на рабочих местах;
- не вносить изменения в настройку средств защиты информации, не изменять и не тиражировать программное обеспечение;
- не осуществлять самостоятельно дополнительную установку каких-либо программных и/или аппаратных средств на персональные компьютеры;
- использовать аппаратные и программные средства только в служебных целях;
- 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.

13 Учет лиц, допущенных к персональным данным, обрабатываемым в информационных системах

Допуск к персональным данным, обрабатываемым в информационной системе, лицам, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей, должен производиться в соответствии с порядком, установленным разрешительной системой доступа.

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

Ведение разрешительной системы доступа возложено на отдел развития информационных ресурсов Учреждения.

Основанием для обеспечения доступа к персональным данным, обрабатываемых в информационных системах, и включения должностных лиц в разрешительную систему доступа являются сведения, подаваемые руководителями структурных подразделений оператора.

14 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 выдаются 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 русского, английского алфавита;

- строчные буквы русского, английского алфавита; цифры (от 0 до 9).

4) Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

5) Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

6) Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

7) Запрещается выбирать пароли, которые уже использовались ранее.

Обязательным требованием организации парольной защиты является полная плановая смена паролей в информационных системах персональных данных не реже одного раза в 3 месяца. Ответственным за проведение плановой смены паролей является лицо, ответственное за обеспечение безопасности персональных данных.

Правила ввода пароля:

- ввод пароля осуществляется с учетом регистра, в котором пароль был задан;
- во время ввода паролей исключается возможность его подсматривания посторонними лицами или техническими средствами.

Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Лица, допущенные к обработке персональных данных в информационных системах Учреждения, обязаны:

- четко знать и строго выполнять требования организации парольной защиты;
- своевременно сообщать должностному лицу, ответственному за обеспечение безопасности персональных данных, об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Запрещается:

- вести разговоры с посторонними лицами о процедурах доступа к информационным системам и информации;
- набирать на клавиатуре при посторонних лицах персональный пароль и записывать его;
- сообщать устно или письменно свой персональный пароль.

15 Использование ресурсов сети Интернет

Подключение информационных систем персональных данных к сетям общего доступа и (или) международного обмена (сети Интернет и других), 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 производится 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 организации доступа к сети Интернет на конкретных компьютерах принимается руководителем Учреждения на основании сведений, представленных руководителем структурного подразделения.

Почтовый обмен с сетью Интернет организуется 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:

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

При работе в сети Интернет запрещается:

- осуществлять работу при отключенных средствах защиты;
- передавать по сети Интернет защищаемую информацию без использования средств шифрования;
- скачивать из сети Интернет программное обеспечение и другие файлы;
- посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО, сайты с подозрительным контентом и другие);
- нецелевое использование подключения к сети Интернет.

16 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 Учреждения.

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

3. Все возможные каналы поступления вредоносных программ в информационно-технологическую инфраструктуру Учреждения анализируются и защищаются средствами антивирусной защиты.

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

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

6. Любые средства вычислительной техники, используемые в Учреждения, в ходе эксплуатации подвергаются непрерывному антивирусному мониторингу и сканированию.

17 Организация антивирусной защиты в Учреждении

Администрирование средств антивирусной защиты информационных систем персональных

данных, конфигурирование и определение политик работы клиентских модулей, системный мониторинг возлагаются на отдел развития информационных ресурсов Учреждения.

Действия пользователей по обеспечению антивирусной защиты при повседневной деятельности:

1. Обязательной антивирусной проверке подвергается любая информация, получаемая пользователем из сети Интернет посредством электронной почты, путем загрузки с веб-сайтов либо иным доступным способом.

2. Антивирусной проверке подвергаются все съемные носители информации (дискета, флеш-память, компакт-диск и пр.) перед подключением к персональному компьютеру.

3. Запрещается посещать сайты с потенциально опасным программным обеспечением (сайты с подозрительным контентом).

4. Запрещается открывать файлы, полученные по электронной почте от неизвестного отправителя или вызывающие подозрения.

5. Запрещается установка и запуск на рабочей станции программ и файлов, полученных из источников, не предусмотренных технологией обработки информации или не предназначенных для выполнения пользователем своих функциональных обязанностей.

6. Пользователям запрещается влиять на работоспособность средств антивирусной защиты (отключать антивирусную защиту, изменять параметры антивирусной защиты, изменять настройки межсетевых экранов и пр.).

7. О любых ошибках в работе средств антивирусной защиты следует немедленно сообщать в отдел развития информационных ресурсов Учреждения.

8. При получении от отдела развития информационных ресурсов Учреждения сообщения о распространении вирусной эпидемии и инструкции по предотвращению, необходимо принять меры по выполнению требований инструкции, по недопущению заражения рабочей станции, проникновения вирусов в информационно-технологическую инфраструктуру Учреждения.

Действия пользователей при обнаружении вируса:

1. К основным признакам проявления вирусов относятся:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;

- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

2. Вирус может быть обнаружен как при проверке полученного по электронной почте или иным способом подозрительного файла либо съемного машинного носителя информации на вирусы, так и при сканировании системы антивирусной программой в «прозрачном» для пользователя режиме. Предупреждения об обнаружении вируса отображаются в виде всплывающего окна.

3. При обнаружении или наличии подозрения на присутствие вирусного программного обеспечения на автоматизированном рабочем месте (персональном компьютере пользователя) пользователь обязан немедленно сообщить об этом в отдел развития информационных ресурсов Учреждения и прекратить работу на персональном компьютере.

4. Запрещается самостоятельное «лечение» зараженных файлов, персональных компьютеров, съемных носителей. Все необходимые антивирусные процедуры проводятся специалистами отдела развития информационных ресурсов Учреждения.

5. Запрещается перенос информации с помощью внешних носителей на другие компьютеры.

6. Запрещается запускать программы или открывать файлы, в которых был обнаружен вирус.

18 Учет носителей информации

В Учреждения организуется учет внешних носителей персональных данных (далее - защищаемые носители). Учет защищаемых носителей осуществляется специально уполномоченными из числа сотрудников лицами.

Учет всех защищаемых носителей информации производится с помощью их маркировки и занесения учетных данных в журнал учета внешних 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.

19 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.

Проверка наличия учитываемых носителей персональных данных проводится один раз в год лицами, ответственными за обеспечение безопасности персональных данных. В ходе ревизии может быть определен 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.

20 Резервирование информации

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

Резервирование должно осуществляться на различные защищаемые носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий осуществляется в надежных сейфах (металлических шкафах) и в серверных помещениях.

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.

21 Порядок уничтожения персональных данных по достижении цели обработки

В случае достижения цели обработки персональных данных оператор обязан прекратить

обработку персональных данных и уничтожить персональные данные 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 федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные 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 Учреждения.

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 Департамента, включаются в состав электронных архивов и хранятся согласно установленным законодательством срокам отдельно от баз данных информационных систем Учреждения.

22 Контроль состояния обеспечения безопасности персональных данных в Учреждения

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.

Организационный контроль состояния обеспечения безопасности персональных данных в Учреждения проводится в форме внутренних проверок обеспечения безопасности персональных данных. Организационный контроль проводится совместно с сотрудниками структурных подразделений, ответственными за вопросы обеспечения безопасности информации своих подразделениях.

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.

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 услуги по контролю (аудиту) состояния обеспечения безопасности персональных данных.

Непосредственный контроль за выполнением требований законодательства РФ по защите персональных данных при обработке персональных данных осуществляют лица, ответственные за обеспечение безопасности персональных данных.

23 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 Учреждения проводятся периодические проверки условий обработки персональных данных. Проверки осуществляются

лицами, ответственными за обеспечение безопасности персональных данных, комиссией Учреждения.

Проверки осуществляются на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Контролируемые вопросы в ходе проведения проверок:

- наличие у сотрудников 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 итогам каждой проверки составляется протокол, который утверждается директором Учреждения и хранится в течение трех лет. Форма протокола приведена в приложении 5 к настоящему Положению.

При выявлении в ходе проверки нарушений в протоколе указываются мероприятия по устранению нарушений и сроки исполнения. Информация о результатах проверки и мерах, необходимых для устранения выявленных нарушений, докладывается директору Учреждения.

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

24.1 Информирование об инцидентах нарушения информационной безопасности

Все сотрудники незамедлительно информируют начальника отдела и должностное лицо, ответственное за информационную безопасность, об инцидентах нарушения информационной безопасности.

В случае выявления фактов распространения персональных данных или утраты материальных носителей персональных данных руководитель Учреждения принимает решение о проведении служебной проверки.

Комиссия Учреждения 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.

24.2 Информирование о проблемах безопасности

Все сотрудники, осуществляющие обработку персональных данных, должны обращать внимание и сообщать начальнику отдела и должностному 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. При этом не допускается самостоятельный поиск сотрудниками подтверждения подозреваемого недостатка в системе безопасности. Это требование предъявляется в интересах самих сотрудников, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы.

24.3 Информирование о сбоях программного обеспечения

Сотрудники, осуществляющие обработку персональных данных с использованием средств вычислительной техники, 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 Департамента), работа на нем прекращается;
- не допускается перенос информации с помощью внешних носителей на другие компьютеры;
- о проблеме немедленно извещается начальник отдела и должностное лицо, ответственное за информационную безопасность.

Пользователям запрещается пытаться самостоятельно удалить подозрительное программное обеспечение. Ликвидация последствий сбоев осуществляется специалистами учреждения.

24.4 Реагирование на факты разглашения персональных данных

По каждому факту разглашения персональных данных или утраты материальных носителей персональных данных руководитель Учреждения принимает решение о проведении служебной проверки.

По факту утечки сведений из информационных систем персональных данных в состав комиссии, проводящей служебную проверку, обязательно включается представитель отдела развития информационных ресурсов Министерства.

25 Ответственность за разглашение персональных данных

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 Учреждения.

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

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

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

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.