БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВОРОНЕЖСКОЙ ОБЛАСТИ
«ЦЕНТР КОМПЛЕКСНОЙ РЕАБИЛИТАЦИИ ИНВАЛИДОВ
«СЕМЬ СТУПЕНЕЙ»

ПРИКАЗ

от « 09 » 04/ 2024 г. № 162 /од

г. Воронеж

Об организации работ по обеспечению безопасности персональных данных

С целью организации работ по обеспечению безопасности персональных данных и во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

п р и к а з ы в а ю:

1. Утвердить прилагаемый Перечень должностей работников учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

2. Утвердить прилагаемое Положение (с приложениями) об обработке и защите персональных данных.

3. Возложить выполнение работ по обеспечению безопасности персональных данных и поддержанию достигнутого уровня защиты персональных данных на этапах эксплуатации информационных систем персональных данных, методическое руководство и координацию работ по обеспечению безопасности персональных

данных при их обработке в информационных системах учреждения на отдел первичного приема и информационных технологий (Щербатых А.Н.).

4. Ответственность за выполнение правил обеспечения безопасности персональных данных в отделах и отделениях учреждения возложить на начальников отделов и заведующих отделениями.

5. Признать утратившим силу приказ от 26.12.2023 № 220/ОД «Об организации работ по обеспечению безопасности персональных данных».

6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор И.А. Гринева

Приложение № 1

УТВЕРЖДЕНО
приказом БУ ВО «Семь «Ступеней»

от 09.04.2024 № 162/од

Перечень должностей работников БУ ВО «ЦКРИ «Семь Ступеней», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Административно-управленческий персонал

1.1. Руководители

– Директор
– Заместитель директора (по общим вопросам)
– Заместитель директора (по реабилитации)
– Заместитель директора
– Главный бухгалтер

1.2. Руководители структурных подразделений

– Заведующий отделением социально-медицинских услуг – врач
– Заведующий отделением организационно-методической работы
– Заведующий отделением социально-психологической реабилитации
– Заведующий отделением социальной реабилитации и адаптивной физической – культуры
– Заведующий отделением профессиональной реабилитации
– Заведующий отделением комплексной реабилитации участников СВО
– Заведующий отделением сопровождаемого проживания (учебная квартира)
– Начальник отдела первичного приема и информационных технологий
– Начальник отдела материально-технического обеспечения и хозяйственной деятельности

2. Основной персонал

– Заместитель главного бухгалтера
– Бухгалтер
– Экономист
– Специалист по кадрам
– Юрисконсульт
– Делопроизводитель

3. Отдел первичного приема и информационных технологий

– Заместитель начальника отдела

– Социолог
– Инженер-электроник
– Специалист по социальной работе

4. Отделение организационно-методической работы
– Специалист по социальной работе
– Методист
– Специалист по профессиональной ориентации инвалидов

5. Отделение социально-психологической реабилитации
– Педагог – психолог
– Психолог
– Логопед
– Специалист по социальной работе (механотерапия)

6. Отделение социальной реабилитации и адаптивной физической культуры
– Специалист по реабилитационной работе в социальной сфере
– Педагог-организатор
– Педагог дополнительного образования

7. Отделение профессиональной реабилитации
– Методист
– Преподаватель

8.Учебно - производственные мастерские
– Старший мастер производственного обучения
– Мастер производственного обучения

9. Отделение социально-медицинских услуг (со стационаром)
– Врач–невролог
– Врач–терапевт
– Врач–физиотерапевт
– Врач–психиатр
– Врач–психотерапевт
– Врач–травматолог–ортопед
– Медицинская сестра по физиотерапии
– Медицинская сестра процедурной
– Медицинская сестра палатная
– Медицинская сестра по массажу

10. Отделение комплексной реабилитации участников СВО

– Специалист по социальной работе
– Психолог
– Социальный работник
– Медицинский психолог

11. Отделение сопровождаемого проживания (учебная квартира)

– Социальный работник
– Специалист по социальной работе
– Психолог

12. Отдел материально-технического обеспечения и хозяйственной деятельности

– Заведующий хозяйством
– Заведующий складом
– Комендант

Приложение № 2

УТВЕРЖДЕНО
приказом БУ ВО «Семь «Ступеней»

от 09.04.2024 № 162/од

ПОЛОЖЕНИЕ

об обработке и защите персональных данных

в БУ ВО «ЦКРИ «Семь Ступеней»

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 персональных данных или иного законного основания;

– **обработка персональных данных** – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных;

– **обработка персональных данных без использования 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 субъектов персональных 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** – юридическое лицо (БУ ВО «ЦКРИ «Семь Ступеней») или физическое лицо (сотрудник учреждения), организующие и (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 субъекту персональных данных, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и 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.

Сокращения

Сокращение	Определение
ИС	информационная система
ИСПД	информационная система персональных данных
Комиссия	комиссия по обеспечению безопасности персональных данных БУ ВО «ЦКРИ «Семь Ступеней»
Оператор	БУ ВО «ЦКРИ «Семь Ступеней»
Ответственное лицо	лицо, ответственное за выполнение мероприятий по обеспечению безопасности персональных данных
ПД	персональные данные
ПО	программное обеспечение
Политика	приказ Учреждения «Об утверждении документов, определяющих политику в отношении обработки персональных данных в БУ ВО «ЦКРИ «Семь Ступеней»
Положение	положение об обработке и защите персональных данных в БУ ВО «ЦКРИ «Семь Ступеней»
СВО	специальная военная операция
Учреждение	БУ ВО «ЦКРИ «Семь Ступеней»
ЭП	электронная подпись

1. Общие положения

1.1. Положение об обработке и защите персональных данных в БУ ВО «ЦКРИ «Семь Ступеней» разработано в целях организации обработки персональных данных сотрудников и иных субъектов, персональные данные которых подлежат обработке в БУ ВО «ЦКРИ «Семь Ступеней», 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 документа - приказ Учреждения «Об утверждении документов, определяющих политику в отношении обработки персональных данных в БУ ВО «ЦКРИ «Семь Ступеней» (далее - Политика).

1.3. Положение разработано в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях, Гражданского кодекса Российской Федерации, Федеральных законов Российской Федерации от 27.07.06 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.06 г. № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 21.03.12 г. № 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 01.11.12 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.08 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 от 11.02.13 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18.02.13 г. № 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.

1.4. Целью организации обработки персональных данных и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения является обеспечение конституционных

прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.5. 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;
- 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;
- Учреждение должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством;
- обеспечение защиты прав и свобод 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;
- соответствие обязанностей по обработке персональных данных действующему законодательству и иными нормативными актами по персональным данным;
- принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных;
- недопустимость ограничения прав и свобод гражданина по мотивам, связанным с использованием различных способов обработки персональных данных;
- недопустимость использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах Учреждения, конкретному субъекту персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;

- документального оформления всех принятых решений по обработке персональных данных.

1.6. 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 ПД

3.1. Обработка персональных данных в Учреждении должна осуществляться на законной и справедливой основе.

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

– издание Учреждением документов по вопросам обработки и защиты персональных данных;

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

– определение списка 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 требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

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

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

– опубликование на официальном сайте Учреждения в информационно-телекоммуникационной сети Интернет документов, определяющих политику Учреждения в отношении обработки персональных данных;

– осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону Российской Федерации от 27.07.06 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Учреждения в отношении обработки персональных данных, локальным актам Учреждения.

4. Порядок обработки ПД в Учреждении

4.1. Цели обработки персональных данных

Цели обработки персональных данных в Учреждении определены в документе – приказ Учреждения «Об утверждении документов, определяющих политику в отношении обработки персональных данных в БУ ВО «ЦКРИ «Семь Ступеней».

4.2. Состав персональных данных

4.2.1. Состав (объем и содержание) персональных данных определяется нормативными правовыми актами, устанавливающими порядок предоставления услуг клиентам, кадрового, бухгалтерского учета, иными документами, регламентирующими порядок деятельности Учреждения. Состав персональных данных не должен превышать перечень информации, необходимой для реализации конкретных функций.

4.2.2. Субъектами персональных данных, сведения о которых обрабатываются в Учреждении в собственных ИС, являются клиенты – граждане, обратившиеся за получением социальных услуг;

Для перечисленных субъектов персональных данных Учреждение выполняет функции Оператора.

4.2.3. Оператор получает сведения о персональных данных субъекта из следующих источников:

– информация, представляемая клиентом при обращении в Учреждение: документ, удостоверяющий личность, документы МСЭ (ИПРА, ПРП, справка), страховое свидетельство обязательного пенсионного страхования (СНИЛС), другие документы, установленные порядком регистрации клиента в Учреждении;

– иные документы и сведения, предоставляемые субъектом персональных данных.

4.3. Условия и порядок обработки персональных данных

4.3.1. Обработка ПД – 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), блокирование, удаление, уничтожение персональных данных.

Обезличивание персональных данных в учреждении не осуществляется.

4.3.2. Обработка ПД 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.

Типовая форма согласия субъекта или его законного представителя на обработку персональных данных приведена в документе Политика, а также в Приложениях 6 - 7 к настоящему Положению.

В случае отказа предоставить персональные данные Оператор обязан разъяснить субъекту персональных данных или его законному представителю юридические последствия отказа предоставления персональных данных. Форма разъяснения представлена в Политике.

4.3.3. Получение ПД 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.

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

Состав должностных лиц, имеющих доступ к обработке персональных данных, а также состав лиц, допущенных к ресурсам ИСПД определяется приказами руководителя Учреждения.

Внутри Учреждения к разряду потребителей ПД, помимо руководителя и его заместителей, относятся те сотрудники структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей.

Приказом Учреждения определен Перечень должностей работников БУ ВО «ЦКРИ «Семь Ступеней», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение № 1 к приказу «Об организации работ по обеспечению безопасности персональных данных»).

4.3.5. 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.

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

4.3.7. 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, соблюдении правил их

обработки, а в случае расторжения трудового договора обязательства прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей. Типовая форма обязательства приведена в Политике.

4.4. Способы обработки персональных данных

Обработка персональных данных подразделяется на:

– обработка персональных данных, осуществляемая в автоматизированном режиме (в ИС);

– обработка персональных данных, осуществляемая без использования средств автоматизации.

4.5. Обработка персональных данных, 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 персональных данных (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; наименовании Учреждения; фамилию, имя, отчество субъекта 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.

Формы документов, применяемые при обработке персональных данных без использования средств автоматизации, в рамках предоставления социальных услуг клиентам Учреждения:

- документ «Карта получателя услуг» (для инвалида), «Личное дело» (для участника СВО), «Карточка клиента» (для клиента отделения сопровождаемого проживания);
- документ «Индивидуальная программа предоставления социальных услуг»;
- документ «Медицинская карта»;
- необходимые медицинские справки (например, справка об эпидокружении);
- справка о среднедушевом доходе;
- договор на предоставление социальных услуг;
- иные формы документов необходимых для достижения цели.

4.6. 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 01.11.12 № 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 01.11.12 № 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.

ИС Учреждения:

- «База данных оказания услуг».

Внешние ИС:

- Единая централизованная информационная система Воронежской области по бюджетному учету и отчетности;

- Единая информационная система персонифицированного учета граждан в органах социальной защиты Воронежской области;
- Федеральный реестр медицинских работников.

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. Форма журнала приведена в Приложении 2 к настоящему Положению.

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:

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

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

3) подпись субъекта персональных данных или его 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 в течение срока действия трудового договора. После увольнения работника Учреждение продолжает хранить его ПД. Это необходимо, чтобы начислить, удержать и перечислить налоги за последний месяц работы, отчитаться в фонды и налоговую инспекцию и т.д.

Сроки хранения ПД в Учреждении установлены в соответствии с «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», утвержденным приказом Федерального архивного агентства от 20.12.2019 № 236.

Персональные данные, связанные с предоставлением социальных услуг, обрабатываются и хранятся до достижения цели их обработки либо до отзыва субъектом персональных данных своего согласия.

4.9. Лицо, ответственное за выполнение мероприятий по обеспечению безопасности персональных данных

Приказом руководителя Учреждения назначается лицо, ответственное за выполнение мероприятий по обеспечению безопасности персональных данных - Ответственное лицо.

Ответственное лицо получает указания непосредственно от директора (ответственный за организацию обработки ПД) или от Администратора информационной безопасности (ответственный за организацию мероприятий по обеспечению безопасности ПД).

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 работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

5. Общая характеристика собственных ИСПД

В целях учета оказанных социальных услуг используется ИС «База данных оказания услуг». Применяется смешанная обработка персональных данных. Для автоматизации обработки применяется ПО «1С:8.3. БД оказания услуг».

ИС содержит следующие категории персональных данных:

- фамилия, имя, отчество;
- дата рождения;
- пол;
- адрес регистрации;
- контактные телефоны;
- данные документа, удостоверяющего личность;
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);
- данные документа «Индивидуальная программа реабилитации или абилитации инвалида»;
- данные документа «Программа реабилитации пострадавшего в результате несчастного случая на производстве и профессионального заболевания»;
- данные документа «Справка МСЭ»;
- данные документа «Индивидуальная программа предоставления социальных услуг»;
- сведения о состоянии здоровья;
- данные документа «Справка о среднедушевом доходе»;
- сведения о последнем месте учебы, работы (профессия, должность);
- данные документов об образовании, квалификации, профессиональной подготовке;
- иные персональные данные необходимые для достижения цели.

6. Обеспечение безопасности персональных данных

6.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью 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.

6.2. 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.

6.3. Организация и проведение работ по обеспечению безопасности персональных данных в Учреждении 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).

6.4. 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 ИСПД в целях:

– предотвращения возможных (потенциальных) угроз безопасности;

– нейтрализации реализуемых угроз безопасности;

– ликвидации последствий реализации угроз безопасности и восстановления нормального функционирования ИСПД.

6.5. 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 ИСПД.

7. Организационная структура системы обеспечения безопасности персональных данных

7.1. Планирование, управление и координация деятельности Учреждения по обеспечению безопасности персональных данных осуществляются Администратором информационной безопасности.

7.2. Выполнение мероприятий по обеспечению безопасности персональных данных и поддержанию достигнутого уровня защиты персональных данных на этапах эксплуатации информационных систем персональных данных в Учреждении возложены на ответственного за выполнение мероприятий по обеспечению безопасности персональных данных (Ответственное лицо).

7.3. В целях обеспечения безопасности персональных данных Ответственное лицо взаимодействует со всеми структурными подразделениями Учреждения, сотрудники которых имеют доступ к ИСПД.

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

7.5. Ответственность за выполнение правил обеспечения безопасности персональных данных в структурных подразделениях возложена на начальников отделов и заведующих отделениями.

7.6. Комиссия по обеспечению безопасности персональных данных:

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

- приказов по вопросам безопасности персональных данных;
- перечня сведений конфиденциального характера;

– положений, руководств, регламентов и инструкций по вопросам организации и контроля обеспечения информационной безопасности.

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

7.7. Отдел первичного приема и информационных технологий:

7.7.1. 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.

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

– списков сотрудников, допущенных к обработке персональных данных (по подразделениям Учреждения, по информационным системам);

– журнала учета машинных носителей ПД (Приложение 3);

– журнала учета ключевых носителей ЭП (Приложение 4);

– журнала учета выданных паролей (Приложение 5);

– документации на средства защиты информации, включая лицензии, сертификаты.

7.8. Руководители структурных подразделений, ответственные за вопросы обеспечения информационной безопасности в своих подразделениях:

– организуют контроль выполнения мероприятий по защите персональных данных в подразделениях;

– отвечают за своевременное предоставление информации о включении работников своего подразделения в список лиц, допущенных к обработке персональных данных в информационных системах;

– отвечают за своевременное предоставление информации об исключении из списка лиц, допущенных к обработке персональных данных в информационных системах, сотрудников своих подразделений (в связи с увольнением, изменением должностных обязанностей, переводом на другую работу (должность, отдел) и т.д.).

7.9. Администратор информационных систем персональных данных:

– осуществляет администрирование ИСПД Учреждения.

7.10. Пользователи информационных систем персональных данных:

– осуществляют обработку персональных данных в ИСПД 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, установленных 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 журнале учета внешних носителей персональных данных.

8. Порядок доступа сотрудников в помещения, в которых ведется обработка ПД

8.1. Помещения, в которых размещается оборудование, предназначенное для обработки персональных данных в информационных системах, хранятся внешние 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, внешних носителей информации и документов, защиту конфиденциальной информации от несанкционированного доступа. Для этого входные двери этих помещений оборудуются прочными, надежными замками.

8.2. В помещения, 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.

8.3. 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.

8.4. 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.

8.5. 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.

8.6. 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.

8.7. 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.

8.8. 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 Администратором 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.

8.9. Ремонт (вне помещений Учреждения), списание, утилизация (выбытие), реализация и другие действия с оборудованием, на котором обрабатывались или хранились персональные данные, 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 акт.

8.10. Контроль за соблюдением порядка доступа сотрудников в помещения осуществляют руководители структурных подразделений.

9. Организация доступа к персональным данным

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

9.2. Обеспечение конфиденциальности персональных данных не требуется в отношении общедоступных персональных данных.

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

Сотрудники, которым персональные данные необходимы для выполнения должностных обязанностей, подписывают обязательство прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей, в случае расторжения с ними трудового договора. Форма обязательства приведена в Политике.

9.4. Правила и порядок оформления доступа сотрудников к ИСПД, а также порядок разграничения доступа к ним определяются Положением о разрешительной системе доступа к информационным системам персональных данных Учреждения.

9.5. 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 директора Учреждения.

9.6. Доступ сотрудников 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 актами Учреждения, настоящим Положением;

– изменение должностных обязанностей, перевод на другую работу.

10. Организационные меры обеспечения безопасности ПД, 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 прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей, в случае расторжения с ними трудового договора.

При вступлении в должность нового сотрудника руководитель подразделения, в которое 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.

11. Обязанности лиц, допущенных к обработке ПД

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 ИСПД, 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 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 за пределы Учреждения;

– 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.

12. Учет лиц, допущенных к ПД, обрабатываемым в ИС

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 Ответственное лицо.

13. Организация парольной защиты

13.1. В целях обеспечения защиты от несанкционированного доступа к персональным данным и регистрации действий пользователей с персональными данными в ИСПД организуется система парольной защиты.

13.2. Для обеспечения доступа к информационным системам персональных данных всем пользователям устанавливаются личные пароли. Личные пароли доступа к ресурсам информационных систем персональных данных выдаются пользователям Ответственным лицом.

13.3. 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 и (или) английского алфавита;

– строчные буквы русского и (или) 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.

13.4. Обязательным требованием организации парольной защиты является полная плановая смена паролей в информационных системах персональных данных не реже одного раза в полугодие. Ответственным за проведение плановой смены паролей является Ответственное лицо.

13.5. 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.

13.6. 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 логином/паролем.

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

– четко знать и строго выполнять требования организации парольной защиты;

– своевременно сообщать Администратору информационной безопасности 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.

14. Использование ресурсов сети Интернет

При необходимости подключения средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных и другой конфиденциальной информации, к сетям общего доступа и (или) к сети Интернет 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 Администратором информационной безопасности 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 локальным 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) к сети Интернет, не допускается.

При работе в сетях общего доступа и (или) в сети Интернет соблюдаются следующие правила:

1. Работа в сетях общего доступа и (или) в сети Интернет на элементах ИС проводится при служебной необходимости.

2. 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;

– посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое ПО, сайты с подозрительным контентом и другие);

– нецелевое использование подключения к сети Интернет.

15. 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 и персональных компьютерах, используемых в Учреждении и подключенных к сетям общего доступа и (или) к сети Интернет.

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

3. Все возможные каналы поступления вредоносных программ во внутреннюю сеть 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 баз данных вирусов.

16. Организация антивирусной защиты

Администрирование средств антивирусной защиты ИСПД, конфигурирование и определение политик работы клиентских модулей, системный мониторинг возлагаются на отдел первичного приема и информационных технологий.

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 сайтов либо иным доступным способом.

2. Антивирусной проверке подвергаются все съемные носители информации (флеш-память, компакт-диск и пр.) при подключении 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 Администратору информационной безопасности.

8. При получении от отдела развития информационных ресурсов Министерства социальной защиты Воронежской области сообщения о распространении вирусной эпидемии и инструкции по предотвращению, отделу первичного приема и информационных технологий необходимо принять меры по выполнению требований инструкции, по недопущению заражения компьютеров и проникновения вирусов во внутреннюю сеть 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, 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 ПО на автоматизированном рабочем месте (персональном компьютере пользователя) пользователь обязан немедленно сообщить об этом Администратору информационной безопасности и прекратить работу на персональном компьютере.

4. Запрещается самостоятельное «лечение» зараженных файлов, персональных компьютеров, съемных носителей. Все необходимые антивирусные процедуры проводятся специалистами отдела первичного приема и информационных технологий.

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

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

17. Учет носителей информации

В Учреждении организуется учет машинных носителей персональных данных (далее – защищаемые носители). Учет защищаемых носителей осуществляется Ответственным лицом.

Учет внешних (съемных) защищаемых носителей информации производится с помощью их маркировки и занесения учетных данных в журнал учета машинных носителей персональных данных (форма журнала приведена в Приложении 3) с отметкой об их движении (выдаче и возврате).

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

Учет защищаемых носителей информации, встроенных в корпуса средств вычислительной техники, производится с помощью занесения их учетных данных в журнал учета машинных носителей персональных данных (форма журнала приведена в Приложении 3) с отметкой об их местонахождении (инвентарный номер системного блока, в который встроен носитель).

Листы журнала нумеруются, прошиваются и опечатываются.

18. Порядок хранения носителей информации

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

Защищаемые носители с персональными данными хранятся в служебных помещениях, а съемные носители - в надежно запираемых шкафах (сейфах). При этом создаются надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить защищаемые носители с персональными данными из служебных помещений без согласования с Администратором информационной безопасности.

Проверка наличия защищаемых носителей персональных данных проводится один раз в год Администратором информационной 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 присутствии членов Комиссии по обеспечению безопасности персональных данных. В учетном журнале об этом делается отметка со ссылкой на соответствующий акт.

19. Резервирование информации

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

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 устанавливает Администратор информационной безопасности.

Контроль за процессом осуществления резервного копирования защищаемых объектов возлагается на отдел первичного приема и информационных технологий.

20. Порядок уничтожения ПД по достижении цели обработки или при наступлении иных законных оснований

Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований описан в документе Политика.

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

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

21. Контроль состояния обеспечения безопасности ПД

21.1. Основными целями контроля состояния обеспечения безопасности персональных данных являются:

– установление степени соответствия принятых мер по обеспечению безопасности ПД 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.

21.2. Основными задачами контроля являются:

– оценка эффективности проводимых мер по обеспечению безопасности персональных данных;

– анализ причин выявленных нарушений и недостатков в организации обработки 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.

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

21.4. Организационный контроль состояния обеспечения безопасности персональных данных проводится Комиссией по обеспечению безопасности

персональных данных в форме внутренних проверок. Организационный контроль может проводиться совместно с руководителями структурных подразделений, ответственными за вопросы обеспечения безопасности информации в своих подразделениях.

21.5. 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 отдел первичного приема и информационных технологий.

21.6. 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.

21.7. Непосредственный контроль, за выполнением требований законодательства РФ по защите персональных данных при их обработке в структурных подразделениях, осуществляют руководители подразделений.

22. Правила осуществления внутреннего контроля соответствия обработки ПД требованиям к защите ПД

22.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в Учреждении проводятся периодические проверки условий обработки персональных данных. Проверки осуществляются лицами, ответственными за обеспечение безопасности персональных данных, Комиссией Учреждения.

22.2. 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 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.

22.3. По итогам каждой проверки составляется протокол, который хранится у ответственного секретаря Комиссии в течение 3 (трех) лет. Форма протокола приведена в Приложении 1 к настоящему Положению.

22.4. 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.

23. 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 и (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;

– неконтролируемые изменения систем;

– сбои ПО 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.

23.1. Информирование об инцидентах нарушения информационной безопасности

Все сотрудники немедленно сообщают о любых наблюдаемых или предполагаемых инцидентах нарушения информационной безопасности своему непосредственному руководителю и Администратору информационной безопасности.

В случае выявления фактов распространения персональных данных или утраты материальных носителей персональных данных директор 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.

23.2. Информирование о проблемах безопасности

Все работники, осуществляющие обработку ПД, должны обращать внимание и сообщать руководителю подразделения и Администратору информационной безопасности о любых замеченных или предполагаемых недостатках и угрозах в области безопасности персональных данных, в том числе в ИСПД. 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.

23.3. Информирование о сбоях ПО

Сотрудники, осуществляющие обработку ПД 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), работа на нем прекращается;

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

– о проблеме немедленно извещается руководитель структурного подразделения и Администратор информационной безопасности.

Пользователям запрещается пытаться самостоятельно удалить подозрительное ПО. Ликвидация последствий сбоев осуществляется специалистами отдела первичного приема и информационных технологий.

23.4. Реагирование на факты разглашения ПД

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

По факту утечки сведений из ИСПД в состав Комиссии, проводящей служебную проверку, обязательно включается представитель отдела первичного приема и информационных технологий.

24. 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 организацию обработки персональных данных и иной конфиденциальной информации возлагается на директора.

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.

Приложение 1
к «Положению об обработке и защите персональных данных» утвержденному приказом от 09.04.2024 № 162/од

Протокол
проведения проверки условий обработки персональных данных

от _____ № ____
(дата)

Настоящий Протокол составлен в том, что ___.___.20___ комиссией по обеспечению безопасности персональных данных проведена проверка условий обработки персональных в БУ ВО «ЦКРИ «Семь Ступеней».

Тема проверки: _____.

Проверка осуществлялась в соответствии с требованиями _____
_____.
(название документа)

Результаты проверки и решения принятые комиссией по результатам проверки:

Проверено: _____
_____.
Выявленные нарушения: _____
_____.
Меры по устранению нарушений: _____
_____.
Срок устранения нарушений: _____.

Утверждаю:
Председатель комиссии

_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*

Члены комиссии:

_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*
_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*

Приложение 2
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Титульный лист (1 страница обложки)

Журнал регистрации обращений и запросов субъектов персональных данных или их представителей в БУ ВО «ЦКРИ «Семь Ступеней»

Начат «___» _____ 20___ г.
Окончен «___» _____ 20___ г.
На _____ листах

Ответственный за ведение журнала: *должность* _____ / *ФИО должностного лица* /

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

Приложение 3
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Титульный лист (1 страница обложки)

ЖУРНАЛ
учета машинных носителей информации ограниченного доступа (внешних (съемных) и встроенных в корпуса средств вычислительной техники)

Начат «___» _____ 20___ г.
Окончен «___» _____ 20___ г.
На _____ листах

Ответственный за ведение журнала: *должность* _____ / *ФИО должностного лица* /

№ пп	Дата постановки на учет	Тип (внешний / встроенный), ёмкость носителя	Регистрационный / серийный номер	Место хранения *(отдел, кабинет, ответственное лицо)*	Место установки / использования (*кабинет, инв № сист. блока, ответственное лицо*)	Вид движения (*выдача / возврат*) для внешнего носителя	Ответственный пользователь			Снятие с учета			Отметка об уничтожении носителя персональных данных	
							ФИО	Дата	Подпись ответственного лица	Дата	Причина	Подпись ответственного лица	Дата / № акта об уничтожении	Подпись Администратора информационной безопасности
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение 4
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Титульный лист (1 страница обложки)

ЖУРНАЛ
учета ключевых носителей электронных подписей

Начат «___» _____ 20___ г.
Окончен «___» _____ 20___ г.
На _____ листах

Ответственный за ведение журнала: *должность* _____ / *ФИО должностного лица* /

№ пп	Идентификатор носителя	Номер сертификата ключа проверки электронной подписи	Для использования в информацион-ных системах	Отметка о получении		Отметка о выдаче		Отметка об уничтожении ключевых документов
				От кого получены	Дата получения	ФИО пользователя	Дата и подпись	

Приложение 5
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Титульный лист (1 страница обложки)

ЖУРНАЛ
учета выданных паролей для доступа к информационным системам персональных данных

Начат «___» _____ 20___ г.
Окончен «___» _____ 20___ г.
На _____ листах

Ответственный за ведение журнала: *должность* _____ / *ФИО должностного лица* /

Дата	Логин (учетная запись пользователя)	ФИО пользователя	Расписка пользователя в получении пароля
Информационная система персональных данных, для доступа к которой выдаются пароли			

Приложение 6
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Форма согласия
на фото- и видеосъемку и
дальнейшее использование фотоснимков и видеоматериалов

Я, _____,

(фамилия, имя, отчество)

_____,

(адрес)

_____

(паспорт: серия, номер, дата выдачи, кем выдан)

_____,

в соответствии со ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю свое согласие на фото- и видеосъемку и дальнейшее использование фотоснимков и видеоматериалов БУ ВО «ЦКРИ «Семь Ступеней» (далее – Оператор), расположенному по адресу: г. Воронеж, ул. Калининградская, 110 в целях:

- обеспечения безопасных условий жизнедеятельности и совершенствования качества оказания социальных услуг в учреждении (своевременное выявление источников угроз безопасности учреждения и террористической деятельности, обеспечения пожарной безопасности, обеспечение безопасности получателей социальных услуг, работников и иных лиц, находящихся на территории и в здании учреждения, обеспечения соблюдения пропускного режима, предотвращения хищения материальных ценностей, обеспечения исполнения должностных обязанностей и норм трудового законодательства);

- размещения на официальном сайте учреждения, а также на официальных страницах социальных сетей учреждения;

- размещения на информационных стендах учреждения;

- использования на методических объединениях, семинарах, конференциях или в других информационно-методических материалах;

- создания презентаций и видеороликов о деятельности учреждения;

- иных целях, не противоречащих требованиям действующего законодательства;

Я осведомлен(а), что данное согласие не требуется в случаях, когда:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах;

- изображение получено при съемке, которая проводилась в местах, открытых для свободного посещения и/или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных мероприятиях и т.п.).

Перечень действий, на совершение которых дается согласие:

разрешаю Оператору производить с моими персональными данными действия (операции), определенные ст. 3 Федерального закона от 27.07.06 г. № 152-ФЗ, а именно: сбор,

систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение персональных данных.

Обработка моих персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между Оператором и третьими лицами в целях соблюдения моих законных прав и интересов.

Согласие вступает в силу с момента его подписания.

Настоящее согласие на фото- и видеосъемку и дальнейшее использование фотоснимков и видеоматериалов действует до достижения цели использования фото- и видеоматериалов и исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

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

«____» _____ 20___ г. _____ _____

(подпись) *(расшифровка подписи)*

Приложение 7
к «Положению об обработке и
защите персональных данных»
утвержденному приказом
от 09.04.2024 № 162/од

Форма согласия законного представителя на фото- и видеосъемку и дальнейшее использование фотоснимков и видеоматериалов недееспособного гражданина

Я,_____,

проживающий(ая) по адресу:_____

_____,

документ, удостоверяющий личность (паспорт) _____

_____

(серия, номер, дата выдачи документа, наименование выдавшего органа)

являясь законным представителем (опекуном) недееспособного _____

_____

(фамилия, имя, отчество)

на основании ч. 6 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных", п. 2. ст. 15 Федерального закона от 24.04.2008 г. № 48-ФЗ "Об опеке и попечительстве", ст. 152.1 Гражданского кодекса РФ, в целях оказания социальных услуг в стационарной (полустационарной) форме, настоящим даю свое согласие БУ ВО «ЦКРИ «Семь Ступеней» (далее - Оператор), находящемуся по адресу: г. Воронеж, ул. Калининградская, 110, на осуществление фото- и видеосъемки моего подопечного, его творческих работ, включая автоматизированную, а также без использования средств автоматизации обработку фото и видео материалов, сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, блокирование, уничтожение в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», с учетом чести, достоинства, прав и интересов моего подопечного.

Я даю согласие на использование фото- и видеоматериалов с участием моего подопечного в следующих целях:

- публикации на официальном сайте, а также на официальных страницах социальных сетей в сети Интернет;
- размещения на информационных стендах;
- размещения на общественных мероприятиях, участником которых является Оператор;
- публичной трансляции в средствах массовой информации, в т. ч. на телевизионных каналах.

Согласие вступает в силу с момента его подписания.

Оператор может осуществлять обработку фото- и видеоматериалов моего подопечного до момента достижения цели обработки фото- и видеоматериалов и исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

Я вправе отозвать настоящее согласие на съемку и обработку фото- и видеоматериалов моего подопечного посредством письменного заявления.

«____» _____ 20___ г. _____ _____

(подпись законного представителя) *(расшифровка подписи)*