Приложение 1
к приказу от «10» 08 2017 г. №110

УТВЕРЖДАЮ
Главный врач
АУЗ УР «РСП МЗ УР»

_____ А.М. Богданов

«10» 08 2017 г.

Политика АУЗ УР «РСП МЗ УР» по обработке персональных данных

Ижевск, 2017

Содержание

1. Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

Политика АУЗ УР «РСП МЗ УР» по обработке персональных данных (далее – Политика) разработано в соответствии с Конституцией Российской Федерации от 12.12.1993 г., международными договорами Российской Федерации, Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации и нормативно-методическими документами, регламентирующих порядок обеспечения безопасности персональных данных (ПДн):

2.1.Нормативно-правовые акты Российской Федерации:

- Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.2.Нормативно-методические документы ФСТЭК России:

- РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30.03.1992 г.;

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК России от 14.02.2008 г.;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК России от 15.02.2008 г.

2.3. Нормативно-методические документы ФСБ России:

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при и их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России от 21.02.2008 г. №149/54-144;

- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 Центра ФСБ России от 21.02.2008 г. №149/6/6-622.

Целью данного Положения является определение порядка обработки персональных данных (ПДн) в АУЗ УР «РСП МЗ УР», выполнение мероприятий по защите ПДн направленных на обеспечение защиты прав и свобод человека и гражданина (пациентов и сотрудников) при обработке его персональных данных, предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Защита ПДн физических и юридических лиц, сотрудников (субъектов) АУЗ УР «РСП МЗ УР» (оператором) достигается выполнением комплекса организационных мероприятий, применением программного обеспечения и технических средств, с целью обеспечения конфиденциальности, целостности и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

Объектами защиты в АУЗ УР «РСП МЗ УР» являются персональные данные, средства и системы информатизации (средства вычислительной техники (СВТ), автоматизированные системы различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства изготовления, тиражирования документов, аудио и видео- записывающие устройства и другие технические средства обработки информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное

программное обеспечение), используемые для обработки ПДн.

Настоящая Политика вступает в силу с момента ее утверждения и является обязательной для исполнения всеми работниками, имеющими доступ к персональным данным.

Все изменения в Политику вносятся приказом.

Все работники АУЗ УР «РСП МЗ УР», обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящей Политикой под подпись.

Обрабатываемые персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных в отношении персональных данных субъектов АУЗ УР «РСП МЗ УР» снимается в случаях утраты практического значения, обезличивания или по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии, если иное не определено законом.

3. Персональные данные, подлежащие защите

К персональным данным субъектов АУЗ УР «РСП МЗ УР» относятся сведения утвержденные перечнем.

Обработка персональных данных осуществляется оператором с целью оказания медицинских услуг и осуществления трудовых отношений с работниками.

Оператор в своих полномочиях осуществляет обработку персональных данных, как с использованием средств автоматизации, так и без их использования.

Информационные ресурсы, содержащие ПДн, расположены в информационных системах персональных данных (ИСПДн) на средствах вычислительной техники (далее – СВТ), состоящих из автоматизированных рабочих мест (АРМ) пользователей на базе персональных электронно-вычислительных машин, серверов хранения данных и съемных носителях информации (HDD, Flash-накопители).

В целях информационного обеспечения в АУЗ УР «РСП МЗ УР» могут создаваться общедоступные источники персональных данных (в том числе справочники, телефонные книги, адресные книги, размещение на сайте АУЗ УР «РСП МЗ УР» информации о медицинском персонале, его квалификации, должности, режиме работы и т.д.). Режим конфиденциальности персональных данных для общедоступных источников персональных данных не устанавливается.

Персональные данные, обработка которых осуществляется без использования средств автоматизации, обособляются от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

При принятии решений, затрагивающих интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Субъекты персональных данных

В соответствии с разделом 3 настоящей Политики к субъектам персональных данных относятся следующие категории лиц:

- граждане, обращающиеся за услугами;
- сотрудники;
- кандидаты для приема на работу.

Все персональные данные субъекта персональных данных оператору следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо АУЗ УР «РСП МЗ УР» должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

АУЗ УР «РСП МЗ УР» не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни, за исключением случаем предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» и Трудовым кодексом Российской Федерации от 30.12.2001 г. №197-ФЗ.

Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» и возможна только с согласия субъекта.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу.

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

Субъект персональных данных имеет право на получение следующей информации:

- подтверждение факта обработки персональных данных оператором;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» или другими федеральными законами.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка.

Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» или иным образом нарушает его права и свободу, субъект персональных данных вправе обжаловать действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

5. Порядок сбора, хранения и использования персональных данных

Субъекты персональных данных должны быть ознакомлены с перечнем сведений, целями и задачами сбора, хранения и использования персональных данных.

Персональные данные субъектов персональных данных могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

Ввод персональных данных в ИСПДн осуществляется работниками, имеющими доступ к работе с персональными данными согласно списку лиц, и в соответствии с их должностными обязанностями. На бумажном носителе информации, содержащей персональные данные, работники, осуществляющие ввод данных, оставляют отметку о дате ввода информации и о лице, осуществившем ее ввод.

Сотрудники, осуществляющие ввод и обработку данных, несут ответственность за достоверность и полноту введенной информации.

При работе с программными средствами, реализующими функции просмотра и редактирования персональных данных, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующих должностных обязанностей.

Хранение персональных данных в ИСПДн осуществляется на СВТ АУЗ УР «РСП МЗ УР» с использованием специализированного программного обеспечения, отвечающего требованиям безопасности.

Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечении установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Хранение резервных и технологических копий баз данных ИСПДн, содержащих персональные данные, осуществляется на сменных носителях информации (HDD, Flash-накопители), доступ к которым ограничен.

Вынос резервных и технологических копий баз данных ИСПДн, содержащих информацию ограниченного доступа, с АУЗ УР «РСП МЗ УР» запрещен. Передача и копирование резервных и технологических копий баз данных допустимо только для прямого использования с целью технологической поддержки ИСПДн.

Копировать и делать выписки персональных данных разрешается исключительно в служебных целях.

6. Доступ к персональным данным

Доступ сотрудников к персональным данным, содержащимся как в информационной системе персональных данных АУЗ УР «РСП МЗ УР», так и на бумажных носителях осуществляется согласно списку лиц.

При получении доступа к персональным данным сотрудники подписывают обязательство (соглашение) о неразглашении персональных данных.

Доступ к информационной системе персональных данных разграничен политикой безопасности системы, реализуемой с использованием технических и организационных мероприятий.

Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в ИСПДн. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.

Запрещается использование для доступа к ИСПДн учетных записей других пользователей.

Созданием, удалением и изменением учетных записей пользователей ИСПДн занимается уполномоченный администратор безопасности ИСПДн в соответствии с должностными обязанностями.

Внутренний доступ (доступ внутри АУЗ УР «РСП МЗ УР»).

Перечень лиц, имеющих доступ к персональным данным, определяется перечнем допущенных лиц.

Внешний доступ.

К числу массовых потребителей персональных данных вне АУЗ УР «РСП МЗ УР» можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые организации;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- банки;
- подразделения муниципальных органов управления.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

Сведения о субъекте персональных данных могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением заверенной копии заявления.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

7. Требования по обеспечению защиты ПДн при обработке без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, 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 (например, отдельные анкеты).

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без

использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (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, имя (наименование) и адрес, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором 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 быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

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

АУЗ УР «РСП МЗ УР» обязано обеспечить сохранность персональных данных путем установления мер, исключающих несанкционированный доступ к персональным данным. К таким мерам относятся:

- ограничение перечня лиц, имеющих право доступа и обработки ПДн, и уровня доступа;

- ведение учета выданных персональных данных, ведение журнала и учет выданных ПДн возлагается на ответственного сотрудника;

- реализация особого режима хранения для документов, содержащих персональные данные субъектов.

АУЗ УР «РСП МЗ УР» обеспечивает раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

АУЗ УР «РСП МЗ УР» вправе определить дополнительные меры в целях обеспечения сохранности персональных данных и исключения несанкционированного доступа к персональным данным в своих локальных актах или приказах.

8. Порядок определения класса и уровня защищенности ИСПДн, оценка угроз безопасности ПДн при их обработке в ИСПДн

Определение класса и уровня защищенности ИСПДн проводится в соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30.03.1992 г. и Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

Определение класса и уровня защищенности ИСПДн проводится на этапе создания ИСПДн или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн.

Класс и уровень защищенности ИСПДн определяется с учетом актуальных угроз, категорий и принадлежности накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и средств защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн.

В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс и уровень защищенности, соответствующий наиболее высокому уровню защищенности входящих в нее подсистем.

По результатам классификации ИСПДн оформляется акт классификации автоматизированной системы, утверждаемый руководителем АУЗ УР «РСП МЗ УР».

Класс и уровень защищенности ИСПДн может быть пересмотрен:

- по решению комиссии по определению класса и уровня защищенности на основе проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной ИСПДн;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Выбор и реализация методов и способов защиты ПДн в ИСПДн осуществляются на основе определяемых угроз безопасности персональных данных и в зависимости от класса и уровня защищенности информационной системы.

Выбранные и реализованные методы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Выявление угроз ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

Угрозы безопасности ПДн при их обработке в ИСПДн определяются на основе Постановления Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России от 14.02.2008 г. и «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России от 15.02.2008 г. Угрозы безопасности ПДн, обрабатываемых в ИСПДн, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Кроме того, угрозы могут быть пересмотрены на основе периодически проводимого анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

При использовании средств криптографической защиты информации в ИСПДн для каждой такой ИСПДн должна определяться модель нарушителя безопасности персональных данных. Модель нарушителя определяется на основе руководящих документов ФСБ России «Методических рекомендаций по обеспечению с помощью

криптосредств безопасности персональных данных при и их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России от 21.02.2008 г. №149/54-144 и «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России от 21.02.2008 г. №149/6/6-622. На основе выработанной модели нарушителя для каждой ИСПДн определяется уровень криптографической защиты ПДн, которому должно соответствовать применяемое средство криптографической защиты.

9. Требования по защите ПДн при их обработке в ИСПДн.

9.1. Общие требования к методам и средствам защиты информации

АУЗ УР «РСП МЗ УР» должно соблюдать режим конфиденциальности персональных данных при обработке ПДн, за исключением случаев, когда обеспечение безопасности ПДн не требуется.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

Методы и средства защиты информации осуществляются в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Меры по обеспечению безопасности персональных данных определяются оператором (уполномоченным лицом) в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при и их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России от 21.02.2008 г. №149/54-144 и «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России от 21.02.2008 г. №149/6/6-622.

Основными мерами по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, являются:

- идентификация и аутентификация субъектов и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении Приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Для реализации методов и способов защиты информации могут применяться такие средства защиты информации как средства защиты от несанкционированного доступа, средства криптографической защиты информации, антивирусные средства, межсетевые экраны, системы обнаружения вторжений, специализированные комплексы защиты и анализа защищенности информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

При обработке ПДн в ИСПДн АУЗ УР «РСП МЗ УР» должны соблюдаться следующие требования безопасности:

- ограничение состава работников и регламентация их функциональных обязанностей, для выполнения которых требуется доступ к ПДн;
- осуществлять раздельное хранение ПДн (съемных носителей информации), обработка которых осуществляется в различных целях;
- обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (съемных носителей информации) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;
- применять средства защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- вести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
- осуществлять контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- должна обеспечиваться возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- проводить контроль за выполнением требований по защите персональных данных не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Съемные носители информации (HDD, Flash-накопители) содержащие

персональные данные, утратившие практическое значение должны быть уничтожены физическим путем, с невозможностью восстановления с них информации по соответствующему акту.

9.2. Организационные меры по защите ПДн при их обработке в ИСПДн

9.2.1. Требования к оборудованию помещений и рабочих мест пользователей ИСПДн

Все технические средства ИСПДн АУЗ УР «РСП МЗ УР» должны находиться в пределах контролируемой зоны, исключающих неконтролируемое пребывание посторонних лиц, а также транспортных и технических средств.

Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в помещения лиц, не связанных с обработкой персональных данных или обслуживанием оборудования.

Размещение устройств отображения и печати информации, используемых в составе АРМ пользователей ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами. Кроме того, должны приниматься дополнительные меры, исключающие подобный просмотр (шторы, жалюзи на окнах, непрозрачные экраны).

Неиспользуемые в процессе обработки ПДн устройства ввода/вывода АРМ пользователей ИСПДн (FDD и CD/DVD дисководы, адаптеры Wi-Fi и Bluetooth, а также USB, FireWire и инфракрасные порты) необходимо отключить либо опечатать (опломбировать) в случае, если данные функции нельзя реализовать с помощью средств защиты информации на программном уровне.

В целях предотвращения перехвата управления загрузкой с изменением необходимой технологической информации для получения несанкционированного доступа в операционную среду информационной системы в BIOS необходимо установить загрузку персональных электронно-вычислительных машин с жесткого магнитного диска, установить пароль на вход в BIOS, а также должны быть опечатаны (опломбированы) системные блоки.

9.2.2. Требования к процедуре получения доступа в ИСПДн

Предоставление доступа к ПДн, обрабатываемых в ИСПДн осуществляется на основании списка лиц.

Администратором безопасности ИСПДн должна проводиться периодическая проверка прав пользователей ИСПДн следующим образом:

- проверка прав пользователей должна проводиться на периодической основе или после каждого изменения в системе. При этом проверка прав пользователей, имеющих особые привилегии для доступа в систему должна проводиться с меньшей периодичностью;
- должна быть предусмотрена регулярная проверка адекватности назначенных привилегий с целью исключения получения кем-либо из пользователей излишних прав.

9.3. Технические требования по защите ПДн при их обработке в ИСПДн

Технические требования по защите ПДн при их обработке в ИСПДн, обеспечивающие реализацию подсистем управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от уровня защищенности информационной системы устанавливаются в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативно-методическими документами по защите персональных данных.

9.4. Требования к резервированию

Для обеспечения возможности быстрого восстановления ПДн и средств их обработки, в случае повреждения (утраты) рабочей копии, в ИСПДн должны выполняться

следующие требования:

- резервные копии информационных ресурсов, содержащих ПДн, и инструкции по их восстановлению должны храниться в специально выделенном месте, отдаленном от места обработки самой информации;

- для обеспечения сохранности резервных копий должен быть применен комплекс организационных и технических мер защиты;

- носители, на которые осуществляется резервное копирование, должны регулярно проверяться на работоспособность;

- должны быть предусмотрены регулярные проверки процедур восстановления.

9.5. Обеспечение безопасности ПДн при передаче

При передаче ПДн субъекта должны соблюдаться следующие требования:

- не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина, а также в других случаях, предусмотренных действующим законодательством Российской Федерации;

- предупреждать лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие ПДн, обязаны соблюдать режим конфиденциальности персональных данных;

- разрешать доступ к ПДн только специально уполномоченным на это работникам, при этом указанные работники должны иметь право получать только те ПДн, которые необходимы для выполнения ими должностных обязанностей;

- передавать ПДн субъектов их представителям в порядке, установленном действующим законодательством Российской Федерации, и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями их должностных функций;

- передача ПДн внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

Трансграничная передача ПДн на территорию иностранного государства допускается без согласия субъекта, если на его территории обеспечивается адекватная защита ПДн.

9.6. Обеспечение безопасности при хранении ПДн

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, поэтому для каждой системы ПДн в обязательном порядке устанавливается срок хранения ПДн и осуществляется регулярное уничтожение, а также обезличивание ПДн при наличии такой возможности.

10. Контроль обеспечения безопасности ПДн

С целью своевременного выявления и предотвращения утечки информации, содержащей ПДн, в ИСПДн должен проводиться периодический контроль не реже 1 раза в 3 года состояния защиты ПДн, который заключается в оценке:

- наличия организационно-распорядительных документов и их соответствие;
- соблюдения требований нормативно-правовых документов Российской Федерации, руководящих и нормативно-методических документов по защите ПДн;
- применяемых средств защиты информации в соответствии с их эксплуатационной документацией.

Контроль осуществляется путем проведения плановых и внеплановых проверок.

Все работы по контролю должны проводиться при строгом соблюдении мер безопасности, исключающих разглашение сведений о проводимых работах, местах размещения технических средств и систем, используемых средств защиты информации и возможных каналах утечки информации, содержащей ПДн.

Ответственность за соблюдение безопасности при проведении проверок выполнения требований по защите ПДн возлагается на уполномоченное лицо.

В случаях обнаружения нарушений при обработке ПДн в ИСПДн ответственные за защиту ПДн обязаны:

- немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;
- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности, принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

11. Ответственность

11.1. Ответственность за обеспечение безопасности ПДн

Лица (работники) АУЗ УР «РСП МЗ УР», виновные в нарушении нормативных правовых актов и внутренних актов АУЗ УР «РСП МЗ УР», регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

АУЗ УР «РСП МЗ УР», как владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения, реализующее полномочия владения, пользования, распоряжения персональными данными в пределах, установленных законом, несет ответственность за использование персональных данных. Ограничение прав субъектов на основе использования информации касающейся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни запрещено.

11.2. Ответственность за разглашение информации, содержащей ПДн

Под разглашением информации, содержащей ПДн, понимается действие или бездействие должностных лиц, в результате которых информация, содержащая ПДн, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Утрата документов, содержащих ПДн, – это выход (в том числе и временный) документов из владения ответственного за их сохранность, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали либо могли стать достоянием посторонних лиц.

Разглашение информации, содержащей ПДн, или утрата документов, содержащих

таковую, относится к числу грубых нарушений трудового договора (контракта).

За разглашение информации, содержащей ПДн, утрату документов, содержащих такие сведения, а также за иные нарушения режима конфиденциальности ПДн виновные лица несут дисциплинарную, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

11.3. Ответственность за нарушение требований настоящего Положения

Руководители структурных подразделений АУЗ УР «РСП МЗ УР» несут ответственность за ежегодное доведение до сотрудников настоящей Политики (под подпись) и обеспечение его соблюдения в подразделениях.

Сотрудники АУЗ УР «РСП МЗ УР» несут персональную ответственность за соблюдение настоящего Положения, а также ответственность по действующему законодательству Российской Федерации за разглашение сведений, составляющих ПДн, ставших известными им случайно или по роду работы.