Утверждено
приказом директора ГОАУСОН
«Мурманский КЦСОН»
№ 53 от «03» 02 2020 года

ПОЛОЖЕНИЕ

по организации защиты персональных данных при их обработке в информационных системах персональных данных в государственном областном автономном учреждении социального обслуживания населения «Мурманский комплексный центр социального обслуживания населения»

1. Общие положения

1.1. Настоящее Положение устанавливает требования по организации защиты персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн), а также определяет порядок работы по обеспечению безопасности ПДн и условия их обработки в государственном областном автономном учреждении социального обслуживания населения «Мурманский комплексный центр социального обслуживания населения» (далее - Оператор), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиты ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Закон), постановлением правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и иными нормативными актами, действующими на территории Российской Федерации.

1.3. Основные термины, используемые в настоящем Положении:

- персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъект ПДн), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДН;

- обработка ПДН – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

- автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;

- распространение ПДн – действия, направленные на раскрытие ПДн неопределённому кругу лиц;

- предоставление ПДн – действия, направленные на раскрытие ПДн определённому лицу или определенному кругу лиц;

- блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

- уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн и ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн;

- обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

- информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения директором Оператора и действует бессрочно, до замены его новым Положением.

1.6. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения.

2. Персональные данные, обрабатываемые в ИСПДн Оператора

2.1. В ИСПДн обрабатываются ПДн следующих субъектов ПДн:

2.1.1. Получателей социальных услуг Оператора;

2.1.2. Физические лица — контрагенты Оператора;

2.1.3. Иных физических лиц, ПДн которых обрабатываются у Оператора.

2.2. Данный перечень может пересматриваться по мере необходимости.

2.3. Персональные данные субъектов ПДн включают: фамилию, имя, отчество; место, год и дату рождения; адрес по прописке, адрес проживания

(фактический); паспортные данные (серия, номер паспорта, кем и когда выдан); телефонный номер (домашний, рабочий, мобильный); семейное положение и состав семьи; ИНН; СНИЛС; информацию о доходах, сведения о воинском учете, сведения о социальных льготах и др. сведения.

3. Цели и задачи обработки ПДн Оператором

3.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

3.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

3.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

3.4. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

3.5. Основными целями обработки ПДн является: оказание социальных услуг получателям социальных услуг, исполнение договорных обязательств.

4. Порядок определения защищаемых информационных ресурсов

4.1. В соответствии с действующим законодательством государственное областное автономное учреждение социального обслуживания населения «Мурманский комплексный центр социального обслуживания населения»

является Оператором ПДн и обрабатывает государственные информационные ресурсы, содержащие ПДн, в пределах своих полномочий, установленных в соответствии с федеральным и областным законодательством,

а также организационно-распорядительными документами учреждения (далее - ОРД) в целях обеспечения реализации прав субъектов ПДн.

4.2. В соответствии с ОРД директором Оператора определяется и утверждается содержание, состав и объем обрабатываемых ПДн.

4.3. В соответствии с ОРД директором Оператора определяется и утверждается перечень документов для ИСПДн.

4.4. При проектировании вновь создаваемой или документировании ранее созданной (эксплуатируемой) ИСПДн определяются цели и содержание обработки ПДн, определяемые действующим законодательством, и утверждается перечень обрабатываемых ПДн.

5. Условия проведения обработки ПДн в ИСПДн

5.1. Директором Оператора с целью планирования, разработки и осуществления мероприятий по защите ПДн при их обработке в ИСПДн определяются и распорядительным документом устанавливаются ответственные должностные лица, допущенные к обработке ПДн (далее - Пользователи).

5.2. Пользователи, осуществляющие обработку ПДн в ИСПДн обязаны принимать необходимые организационные и технические меры для их защиты.

5.3. Пользователи или иные лица, на законных основаниях получившие доступ к ПДн, обязаны не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

5.4. Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его персональных данных:

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

5.4.2. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным.

5.4.3. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ.

5.4.4. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются должностным лицом, допущенным к обработке ПДн.

5.4.5. Получение согласия на обработку ПДн осуществляется путем оформления письменного согласия субъекта ПДн на обработку ПДн по форме, установленной Оператором ИСПДн.

6. Обработка ПДн в ИСПДн Оператора

6.1. Обработка ПДн в ИСПДн осуществляется на основании принципов, определенных ст. 5 Закона, с учетом достижения конкретных, заранее определенных и законных целей.

6.2. Не допускается обработка ПДн в ИСПДн, несовместимая с целями сбора ПДн, а также при отсутствии:

- письменного согласия субъекта ПДн на обработку его ПДн;
- утвержденных ОРД о порядке эксплуатации ИСПДн;
- сертифицированных средств защиты;
- регламентации доступа к автоматизированным рабочим местам (далее - АРМ), предназначенным для обработки ПДн в ИСПДн.

6.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора (Пользователи) несут ответственность в соответствии с разделом 13 настоящего Положения.

6.4. ПДн субъектов на бумажных носителях, обрабатываемых Оператором, хранятся в отделах (у сотрудников), имеющих допуск к

обработке соответствующих ПДн. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

6.5. Места хранения документов, содержащих ПДн:

6.5.1. ПДн получателей социальных услуг Оператора (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн клиентов Оператора, носители информации (флеш-карты, CD-диски, и т.п.) размещаются на полках и запираются на ключ.

6.6. Выдача документов для ознакомления осуществляется лицом, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

6.7. При работе с программными средствами автоматизированной системы Оператора, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

6.8. Ввод ПДн, полученных Оператором, в информационную систему осуществляется Пользователями, имеющими доступ к соответствующим ПДн. Пользователи, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

6.9. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствии с Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.10. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

6.11. При неавтоматизированной обработке ПДн на бумажных носителях:

6.11.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;

6.11.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

6.12. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее — типовые формы), должны соблюдаться следующие условия:

6.12.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые

будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

6.12.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, — при необходимости получения письменного согласия на обработку ПДн;

6.12.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

6.12.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

6.13. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.14. Случаи уничтожения, блокирования и уточнения ПДн:

6.15. 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).

6.16. Уточнение ПДн 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 ПДн.

6.17. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

6.17.1. ПДн на бумажных носителях уничтожаются путем шредирования, а также путем утилизации по договору с уполномоченной организацией.

6.17.2. ПДн, размещенные в памяти ПЭВМ уничтожаются путем удаления её из памяти ПЭВМ.

6.17.3. ПДн, размещенные на флеш-карте, CD-диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

6.18. Об уничтожении носителя информации составляется Акт.

6.19. Помещения Оператора, по окончании рабочего дня и отсутствия в них сотрудников должны запираться, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

6.20. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

6.21. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

6.22. В обязанности администратора ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в обязанности администратора ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

6.23. В обязанности администратора ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

6.24. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения, критичных для безопасности ПДн, полномочий у одного лица не рекомендуется совмещать роли Пользователя ИСПДн и администратора ИСПДн в лице одного сотрудника.

6.25. Квалификационные требования и детальный перечень прав и обязанностей администратора ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные должности, должны быть ознакомлены под роспись.

7. Порядок доступа и обеспечение безопасности ПДн

7.1. Допуск Пользователей Оператора для работы на АРМах, предназначенных для обработки ПДн осуществляется в соответствии с утвержденным списком (перечнем) ответственных должностных лиц Оператора, допущенных к работе в ИСПДн на срок выполнения ими соответствующих должностных обязанностей. В случае прекращения полномочий Пользователя (увольнение, смена исполняемых в учреждении функций и др.) производится удаление учётной записи этого Пользователя после его последнего сеанса работы. В случае увольнения Пользователя все

носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

7.2. Оператором установлен разрешительный порядок доступа к ПДн. Пользователям предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

7.3. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником учреждения по согласованию директора Оператора.

7.4. Запись информации, содержащей ПДн, может осуществляться пользователями только на съемные электронные носители информации, учтенные в установленном порядке.

7.5. Пользователи, участвующие в автоматизированной обработке ПДн и имеющие доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несут персональную ответственность за свои действия и обязаны:

7.5.1. Соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

7.5.2. Знать и выполнять правила работы со средствами защиты информации, установленными на АРМах.

7.5.3. Обеспечивать конфиденциальность персональных паролей и сохранность персональных идентификаторов (ключей).

7.5.4. Выполнять требования по организации антивирусной защиты в полном объеме.

7.6. Пользователи обязаны извещать руководителя структурного подразделения Учреждения и администратора ИСПДн в случае:

- утери персонального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей;
- обнаружения нарушений целостности пломб (наклеек, нарушении или несоответствия номеров печатей) на составляющих узлах и блоках АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД);
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМа, выхода из строя или неустойчивого функционирования узлов АРМа или периферийных устройств;
- некорректного функционирования установленных на АРМе средств защиты информации;
- непредусмотренных конфигураций АРМа отводов кабелей и подключенных устройств.

7.7. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМа в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМа;

- осуществлять обработку ПДн в присутствии посторонних лиц, не допущенных к защищаемой информации;

- записывать и хранить ПДн и другую конфиденциальную информацию на неучтенных электронных носителях;

- оставлять АРМ без присмотра во включенном состоянии, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте персональный идентификатор, машинные носители и документы, содержащие защищаемую информацию;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению предпосылок или угроз утечки (неправомерной модификации) ПДн;

- размещать средства отображения информации таким образом, чтобы создавалась возможность визуального считывания информации.

7.8. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с разрешения директора Оператора.

7.9. В случае если сотруднику сторонней организации необходим доступ к ПДн Оператора, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Оператора, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором с субъектом ПДн.

8. Правила антивирусной защиты ИСПДн

8.1. Настоящий раздел определяет требования к организации защиты информационных ресурсов ИСПДн от разрушающего воздействия вредоносного программного обеспечения.

8.2. К использованию на АРМах ИСПДн допускаются только лицензионные антивирусные средства.

8.3. Установка и начальная настройка средств антивирусного контроля на АРМах ИСПДн может осуществляться администратором ИСПДн.

8.4. Администратор ИСПДн осуществляет обновление антивирусных баз с периодичностью, установленной производителем антивирусного ПО, а также контроль их работоспособности.

8.5. Ежедневно в начале работы в режиме автозагрузки должна проводиться антивирусная обработка загруженных данных АРМа.

8.6. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке подвергаться антивирусной обработке. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

8.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки программного обеспечения компьютера или внесения в него изменений, администратором ИСПДн должна быть выполнена антивирусная проверка ИСПДн.

8.8. После установки (обновления) программного обеспечения защиты ИСПДн администратор ИСПДн должен произвести соответствующую запись в «Журнале учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств в ИСПДн» (Приложение № 1 к настоящему приложению).

8.9. На АРМе запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологически процессом обработки информации в ИСПДн.

8.10. При выявлении признаков наличия на АРМе вредоносных программ (нештатная работа программного обеспечения, появления графических и звуковых эффектов, искажений данных, немотивированной утраты массивов данных, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или с привлечением администратора ИСПДн) обязан провести внеочередную антивирусную обработку своего АРМа.

8.11. Ответственность за проведение мероприятий антивирусной защиты на АРМах ИСПДн возлагается на Пользователей.

9. Порядок резервирования информации и восстановления работоспособности технических средств и программного обеспечения ИСПДн, а также средств защиты информации в ИСПДн:

9.1. Для создания резервной копии конфиденциальной информации, обрабатываемой в ИСПДн, используются только учтенные (зарегистрированные) в установленном порядке носители информации.

9.2. Пользователи обязаны осуществлять резервное копирование конфиденциальной информации, в том числе содержащей ПДн, ежедневно.

9.3. Перед резервным копированием Пользователь обязан проверить внешний электронный носитель информации на отсутствие вирусов.

9.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

9.5. Запрещается запись посторонней информации на учтенные электронные носители, предназначенные для копирования информации, содержащей ПДн.

9.6. Ответственность за проведение резервного копирования в ИСПДн возлагается на Пользователей Оператора.

9.7. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения возлагается на администратора ИСПДн.

9.8. Ответственность за проведение мероприятий по восстановлению работоспособности средств защиты информации (далее - СЗИ) возлагается на администратора ИСПДн.

9.9. При использовании съёмных электронных носителей информации с ПДн, к ним предъявляются следующие требования:

9.9.1. Электронные носители информации, содержащие ПДн учитываются в Журнале учета съёмных носителей ПДн, в Журнале учета несъёмных носителей ПДн.

9.9.2. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории ПДн.

9.9.3. Все бумажные носители, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

10. Осуществление внутреннего контроля состояния защиты информации в ИСПДн

10.1. Организация внутреннего контроля процесса обработки ПДн у Оператора осуществляется в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, вызывающих нарушение работоспособности систем информатизации, а также, в целях совершенствования фактического состояния защищенности ПДн.

10.2. Контроль защиты информации осуществляется путем проведения как периодических плановых, так и внеплановых проверок объектов защиты.

Периодические плановые проверки проводятся не реже одного раза в три года.

10.3. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

10.3.1. Соответствия класса ИСПДн условиям, сложившимся на момент проверки.

10.3.2. Обеспечение соблюдения Оператором требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн.

10.3.3. Выполнения требований предписаний на эксплуатацию технических средств и систем, организации электропитания и заземления.

10.3.4. Сохранности печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты.

10.4. Оценка компетентности персонала, задействованного в обработке ПДн.

10.5. Проверка выполнения Пользователями требований по защите ИСПДн от несанкционированного доступа, антивирусной защиты ИСПДн.

10.6. Выявления возможных каналов утечки информации и внешних программно-технических воздействий на информацию, обрабатываемую в ИСПДн.

10.7. Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

10.8. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

10.9. Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

10.10. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.

10.11. Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

10.12. В случае выявления в ходе контроля предпосылок утечки (утраты) защищаемой информации с целью установления обстоятельств их возникновения и причин невыполнения требований по указанию директора Оператора может проводиться служебное расследование.

10.13. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

10.14. Невыполнение предписанных мероприятий по защите ПДн считается предпосылкой утечки (утраты) защищаемой информации.

11. Права субъекта в отношении ПДн, обрабатываемых Оператором

Субъект ПДн имеет право:

- на получение информации от Оператора, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;
- требовать от Оператора уточнения его ПДн, 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 законодательством РФ меры по защите своих прав;
- обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

12. Права и обязанности Оператора ИСПДн

12.1. Оператор ИСПДн вправе:

12.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

12.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ.

12.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

12.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора ИСПДН, предусмотренных законодательством РФ.

12.2. Оператор ИСПДн обязан:

12.2.1. До начала обработки ПДн уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ.

12.2.2. При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

12.2.3. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований обработки ПДн без согласия субъекта ПДн.

12.2.4. При сборе ПДн, предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством РФ.

12.2.5. Если ПДн получены не от субъекта ПДн, Оператор, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн, обязан предоставить субъекту ПДн следующую информацию:

- наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные настоящим Федеральным законом права Субъекта ПДн;
- источник получения ПДн.

12.2.6. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Оператора ИСПДН, предусмотренных законодательством РФ.

12.2.7. При обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

12.2.8. Сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его представителю информацию безвозмездно о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

12.2.9. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя дать в письменной форме мотивированный ответ, содержащий ссылку на положения законодательства РФ, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

12.2.10. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и

предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

12.2.11. Сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

12.2.12. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

12.2.13. В случае достижения цели обработки ПДн прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

1.2.14. В случае отзыва субъектом ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ.

12.2.15. Назначить лицо, ответственное за организацию обработки ПДн.

13. Ответственность за нарушение настоящего положения

13.1. Директор Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

13.2. Сотрудники Оператора (Пользователи) несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

13.3. Сотрудник Оператора (Пользователь) может быть привлечен к ответственности в случаях:

13.3.1. Умышленного или неосторожного раскрытия ПДн;

13.3.2. Утраты материальных носителей ПДн;

13.3.3. Нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн.

13.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, получателям социальных услуг и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.