Утверждено приказом
МБУ «КЦСОН по Курчатовскому району
г. Челябинска»
от «21» октября 2015г. № 664

ПОЛОЖЕНИЕ
Об обработке персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по обработке персональных данных (далее — Положение) муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения по Курчатовскому району города Челябинска» (далее – учреждение) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цель разработки Положения — определение порядка обработки персональных данных сотрудников и получателей социальных услуг учреждения и иных субъектов персональных данных, персональные данные которых, подлежат обработке на основании полномочий учреждения; обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников и получателей социальных услуг учреждения, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии учреждения, если иное не определено законом Российской Федерации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.2. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку

информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 №152-ФЗ «О персональных данных»).

2.3. Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст.2 ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. Информация - сведения (сообщения, данные) независимо от формы их представления (ст.2 ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.5. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.6. 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 (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.7. Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства РФ от 15.09.2008 № 687).

2.8. Оператор - учреждение.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.10. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.11. 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 (ст.3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

III. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Состав персональных данных, обрабатываемых в ИСПДн учреждения, определяется «Перечнем сведений, содержащих персональные данные».

3.2. Документы со сведениями, содержащими персональные данные, обрабатываются в следующих отделах учреждения:

3.2.1. бухгалтерия;

3.2.2. отдел кадров;

3.2.3. отделение социального обслуживания на дому;

3.2.4. отделение срочного социального обслуживания.

3.3. Комплект документов, сопровождающий процесс оформления трудовых отношений сотрудника учреждения при его приёме, переводе и увольнении:

3.3.1. Информация, представляемая сотрудником при поступлении на работу в учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

3.3.1.1. паспорт или иной документ, удостоверяющий личность;

3.3.1.2. трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;

3.3.1.3. страховое свидетельство государственного пенсионного страхования;

3.3.1.4. документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

3.3.1.5. документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

3.3.1.6. свидетельство о присвоении ИНН (при его наличии у сотрудника).

3.3.2. При оформлении сотрудника в учреждение специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка сотрудника», в которой отражаются следующие анкетные и биографические данные сотрудника:

3.3.2.1. общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

3.3.2.2. сведения о воинском учете;

3.3.2.3. сведения о военно-учетной специальности;

3.3.2.4. данные о приеме на работу;

3.3.3. В дальнейшем в личную карточку вносятся:

3.3.3.1. сведения о переводах на другую работу;

3.3.3.2. сведения об аттестации;

3.3.3.3. сведения о повышении квалификации;

3.3.3.4. сведения о профессиональной переподготовке;

3.3.3.5. сведения о наградах (поощрениях), почетных званиях;

3.3.3.6. сведения об отпусках;

3.3.3.7. сведения о социальных гарантиях;

3.3.3.8. сведения о месте жительства и контактных телефонах.

3.3.4. Вся информация копируется в ИСПДн сотрудника учреждения.

3.3.5. У специалиста по кадрам учреждения создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

3.3.5.1. документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по

анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

3.3.5.2. документация по учреждению, работе отделов (положения, должностные инструкции сотрудников, приказы директора учреждения, документы по планированию, учету, анализу и отчетности в части работы с персоналом учреждения).

3.3.6. Комплекс документов, сопровождающий процесс работы с гражданином (получателем социальных услуг, получателем адресной социальной помощи). Информация, представляемая клиентами, либо их представителями в структурные подразделения учреждения, должна иметь документальную форму. Получатели социальных услуг, либо их представители, предъявляют следующие документы:

3.3.6.1. паспорт или иной документ, удостоверяющий личность;

3.3.7. При первичном обращении физического лица в учреждение, сотрудник заполняет карточку получателя социальных услуг, в которой отражаются следующие анкетные и биографические данные:

3.3.7.1. фамилия, имя, отчество;

3.3.7.2. дата рождения;

3.3.7.3. адрес регистрации, проживания;

3.3.7.4. номер телефона;

3.3.7.5. СНИЛС;

3.3.7.6. сведения о составе семьи;

3.3.7.7. семейное, социальное, имущественное положение;

3.3.7.8. доходы;

3.3.7.9. сведения из документов, подтверждающих право на получение мер социальной поддержки;

3.3.7.10. сведения об инвалидности;

3.3.7.11. сведения о состоянии здоровья;

3.3.7.12. иные сведения, необходимые для оказания социальных услуг.

3.3.8. Данные из документов вносятся сотрудниками в электронном виде в ИСПДн. В бумажном виде впоследствии создаются, хранятся и передаются следующие группы документов, содержащие персональные данные получателей социальных услуг учреждения в единичном или сводном виде:

3.3.8.1. личные дела получателей социальных услуг;

3.3.8.2. журналы учета, регистрации.

IV. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Допуск к персональным данным субъекта могут иметь только те сотрудники учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников

отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей».

Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

4.1.1. ознакомление сотрудника с настоящим Положением, инструкцией пользователя информационных систем персональных данных и другими нормативными актами, регулирующими обработку и защиту персональных данных в учреждении, под роспись;

4.1.2. истребование с сотрудника «Обязательства о неразглашении конфиденциальной информации»;

4.1.3. внесение сотрудника в «Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей» и в «Журнал учёта лиц, допущенных к работе с персональными данными в информационных системах персональных данных».

4.2. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

4.3. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

4.4. Любой субъект имеет право, за исключением случаев, предусмотренных законодательством:

4.4.1. на получение сведений об учреждении в соответствии со ст.14 ФЗ РФ от 27.06.2006 №152-ФЗ;

4.4.2. на ознакомление со своими персональными данными;

4.4.3. на уточнение, блокирование или уничтожение своих персональных данных в случае, если они являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленных учреждением целей обработки.

4.5. В случае если учреждение на основании договора поручает обработку персональных данных другому лицу, существенным условием договора должна являться обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

V. ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Учреждение имеет право получать и обрабатывать персональные данные гражданина (получателя социальной услуги, получателя адресной социальной помощи) об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждения, состоянии здоровья, интимной жизни, (пп.4 п.2 ст.10 ФЗ РФ «О персональных данных» от 26.07.2006 № 152-ФЗ) при условии, что обработка данных категорий персональных данных необходима для оказания социальных услуг.

5.2. Учреждение не имеет права получать и обрабатывать персональные данные сотрудников учреждения и других субъектов персональных данных (кроме гражданина (получателя социальной услуги, получателя адресной социальной помощи), об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждения, состоянии здоровья, интимной жизни,

кроме случаев, когда субъект персональных данных дал согласие в письменной форме с указанием данных категорий персональных данных.

5.3. Учреждение вправе обрабатывать (в том числе передавать) персональные данные субъектов только с их письменного согласия, кроме установленных законодательством РФ исключений, в том числе:

5.3.1. обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

5.3.2. обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным Законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5.3.3. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5.3.4. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5.3.5. обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

5.3.6. обработка персональных данных осуществляется в статистических или иных исследовательских целях;

5.3.7. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.4. Все персональные данные субъектов следует получать у них самих или у их законных представителей. Если персональные данные возможно получить только у третьей стороны, то субъект или его законный представитель, должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

5.5. Должностное лицо учреждения должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

5.6. Должностное лицо учреждения должно проверять достоверность персональных данных, сверяя данные, предоставленные субъектом или его законным представителем, с имеющимися у субъекта или его законного представителя документами.

VI. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных может осуществляться в случаях, установленных законодательством Российской Федерации и согласно Устава учреждения в целях:

6.1.1. оказания семьям и отдельным гражданам, попавшим в трудную жизненную ситуацию, помощи в реализации законных прав и интересов, содействия в улучшении их социального статуса и материального положения, а также психологического статуса;

6.1.2. реализации граждан права на социальное обслуживание в государственной системе социальных служб;

6.2. при определении объема и содержания обрабатываемых персональных данных учреждение должно руководствоваться Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами Российской Федерации.

6.3. При принятии решений, затрагивающих интересы субъекта, учреждение не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

6.4. Персональные данные субъектов обрабатываются и хранятся в помещениях учреждения и на учтённых машинных носителях в соответствии с «Инструкцией по учёту машинных носителей».

6.5. Персональные данные субъектов могут быть получены, обработаны и переданы на хранение, как на бумажных носителях, так и в электронном виде – в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

6.6. При использовании типовых форм документов, обрабатываемых без использования средств автоматизации, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

6.6.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы), должны содержать:

6.6.1.1. сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

6.6.1.2. имя (наименование) и адрес учреждения;

6.6.1.3. фамилию, имя, отчество и адрес субъекта персональных данных;

6.6.1.4. источник получения персональных данных;

6.6.1.5. сроки обработки персональных данных;

6.6.1.6. перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

6.6.1.7. общее описание используемых учреждением способов обработки персональных данных.

6.6.2. 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, в тех случаях, когда существует необходимость получения письменного согласия на обработку персональных данных;

6.6.3. 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;

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

6.7. При ведении журналов (реестров, книг) без использования средств автоматизации, содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится учреждение, или в иных аналогичных целях, должны соблюдаться следующие условия:

6.7.1. необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;

6.7.2. способы фиксации и состав информации, запрашиваемой у субъектов персональных данных;

6.7.3. перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);

6.7.4. сроки обработки персональных данных;

6.7.5. сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится учреждение, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

6.8. копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

6.9. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более 1 (одного) раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится учреждение.

VII. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

7.2. Сотрудник, осуществляющий передачу персональных данных, должен уведомить получателей о факте получения ими персональных данных и о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

VIII. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Хранение бумажных документов, электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

8.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизации.

8.3. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

IX. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается учреждением за счет своих средств, если иное не предусмотрено законодательством РФ.

9.2. В учреждении защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

9.2.1. зафиксированные в бумажных документах;

9.2.2. зафиксированные в электронных документах на технических средствах, включая внешние носители;

9.2.3. речевая (акустическая) информация, содержащая персональные данные;

9.2.4. текстовая и графическая видовая информация, содержащая персональные данные;

9.2.5. информация, представленная в виде информативных электрических сигналов, физических полей, содержащая персональные данные.

9.3. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

9.3.1. Проведение организационных мероприятий:

9.3.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

9.3.1.2. ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

9.3.1.3. проведение обучения сотрудников вопросам защиты персональных данных.

9.3.2. Программно-аппаратная защита:

9.3.2.1. разработка модели угроз безопасности персональным данным;

9.3.2.2. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании» оценку соответствия;

9.3.2.3. организация учёта носителей персональных данных.

9.3.3. Инженерно-техническая защита:

9.3.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

9.3.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

9.4. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за обеспечение безопасности персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами учреждения.

9.5. Организацию и контроль защиты персональных данных в структурных подразделениях учреждения осуществляют их непосредственные руководители.

X. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

10.1. При обработке персональных данных в информационной системе должно быть обеспечено:

10.1.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

10.1.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

10.1.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

10.1.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

10.1.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

10.2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

10.2.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

10.2.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

10.2.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

10.2.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

10.2.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

10.2.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

10.2.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

10.2.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

10.2.9. 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;

10.2.10. описание системы защиты персональных данных.

10.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на администратора безопасности ИСПДн учреждения.

10.4. Список лиц, имеющих доступ к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается приказом руководителя учреждения.

10.5. Сотрудники учреждения, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за обеспечение безопасности персональных данных.

10.6. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

10.7. Иные требования по обеспечению безопасности информации и средств защиты информации в учреждении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

XI. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Состав информационных систем персональных данных учреждения и их характеристика определяется «Перечнем информационных систем персональных данных».

11.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

11.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

11.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

11.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

11.6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также

исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11.7. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн (администратор безопасности ИСПДн).

11.8. При обработке персональных данных в информационной системе должно быть обеспечено:

11.8.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

11.8.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

11.8.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

11.8.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11.8.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

11.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

11.9.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

11.9.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

11.9.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

11.9.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

11.9.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

11.9.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

11.9.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

11.9.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

11.9.9. 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;

11.9.10. описание системы защиты персональных данных.

XII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Сотрудники учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

12.2. Директор учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

12.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

12.4. Сотрудник учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

XIII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Настоящее Положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

13.2. Все сотрудники учреждения, участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.