



ПОЛОЖЕНИЕ

о порядке организации обработки и обеспечении безопасности персональных данных пациентов в информационных системах государственного бюджетного учреждения здравоохранения «Самарская областная клиническая психиатрическая больница»

Самара 2022

Содержание

1	Общие положения.....	3
2	Основные понятия персональных данных	4
3	Персональные данные пациентов	6
4	Сбор, обработка и хранение персональных данных	10
5	Передача персональных данных субъектов ПД.....	14
6	Защита персональных данных	15
7	Заключительные положения	17
8	Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных	17

1 Общие положения

1.1 Настоящее Положение разработано на основании: Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»; Налогового кодекса Российской Федерации (часть вторая); Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»; Приказа Минздравсоцразвития Российской Федерации от 25.01.2011 № 29н «Об утверждении порядка ведения персонифицированного учета в сфере обязательного медицинского страхования.

1.2 Настоящим Положением определяется порядок обращения с персональными данными пациентов (субъектов персональных данных), которые обращаются в государственное бюджетное учреждение здравоохранения «Самарская областная клиническая психиатрическая больница» (далее - Учреждение) в следующих целях: для установления медицинского диагноза, оказания медицинских и медико-социальных услуг, медико-профилактические цели; осуществления статистических и исследовательских целей; исполнения договора о предоставлении платных медицинских услуг; информирования по каналам связи; ведения персонифицированного учета сведений о застрахованных лицах и предоставления счетов (реестров счетов) за оказанную медицинскую помощь; обеспечения финансово-хозяйственной деятельности; контроля количества и качества выполняемой работы; обмена информацией с медицинскими и страховыми организациями, министерством здравоохранения Самарской области, министерством здравоохранения Российской Федерации.

1.3 В отношении сведений о субъектах персональных данных, позволяющих идентифицировать его личность, за исключением обезличенных и общедоступных персональных данных, в установленных федеральными законами случаях, должна обеспечиваться конфиденциальность таких сведений.

1.4 Хранение персональных данных Учреждением осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, если иное не предусмотрено федеральным законом.

1.5 Обработка персональных данных в Учреждении осуществляется как автоматизированным способом в информационных системах персональных данных, так и без использования средств автоматизации (на бумажных носителях).

1.6 Учреждение не осуществляет трансграничную передачу персональных данных и не принимает решения в отношении субъекта персональных данных, основанные исключительно на автоматизированной обработке.

1.7 Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном Федеральным Законом и другими нормативными документами Российской Федерации.

1.8 Положение является обязательным для исполнения всеми работниками Учреждения, имеющими доступ к персональным данным.

1.9 Настоящее Положение не распространяется на отношения, возникающие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.10 В случаях, не указанных в настоящем Положении, следует руководствоваться действующими федеральными законами и нормативными правовыми актами Российской Федерации, регулирующими порядок обработки персональных данных.

1.11 Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения и действует бессрочно, до замены его новым Положением.

1.12 Все изменения в Положение вносятся приказом.

1.13 Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

2 Основные понятия персональных данных

Для целей настоящего Положения используются следующие основные понятия:

- **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

- **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **врачебная тайна** – соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении;
- **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- **документы, содержащие персональные сведения пациента** – формы медицинской и иной учетно-отчетной документации, включающие сведения о персональных данных;
- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения и не раскрывать третьим лицам персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- **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 действия (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – персональные данные), считается **осуществленной без использования средств**

автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

- **общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- **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 (государственное бюджетное учреждение здравоохранения «Самарской области «Самарская областная клиническая психиатрическая больница»»);

- **пациент** – физическое лицо (субъект), обратившееся в Учреждение с целью получения медицинского обслуживания, либо состоящее в иных гражданско-правовых отношениях с Учреждением по вопросам получения медицинских услуг.

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

- **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **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;

3 Персональные данные пациентов

3.1 В соответствии с целями обработки персональных данных ГБУЗ СОКПБ осуществляется обработка следующих персональных данных:

3.1.1 Граждане, обратившиеся за медицинской помощью:

- ФИО;
- дата рождения;
- место рождения;

- пол;
- адрес регистрации;
- адрес проживания;
- данные документа, удостоверяющего личность;
- наименование органа, выдавшего документ, удостоверяющий личность;
- дата выдачи документа, удостоверяющего личность;
- ИНН;
- СНИЛС;
- сведения об образовании;
- место работы;
- адрес электронной почты;
- сумма;
- дата постановки на учет;
- дата снятия с учета;
- данные полиса добровольного медицинского страхования;
- данные медицинского страхового полиса;
- номер медицинской карты;
- сведения о состоянии здоровья;
- диагноз;
- сведения о заболевании;
- сведения о наличии инвалидности;
- результаты медицинского обследования;
- данные лабораторных исследований;
- сведения, указанные в анамнезе;
- сведения, указанные в эпикризе;
- сведения об оказанной медицинской помощи;
- группа крови, резус принадлежность;
- антропометрические данные;
- сведения об оперативных вмешательствах;
- данные исследования;
- медицинское заключение;
- результат обращения за медицинской помощью;
- вид оплаты;
- вид услуги;
- выписка из истории болезни;
- выписка из истории болезни;
- дата оказания услуги;
- дата смерти;

- информация о явках;
- номер истории болезни;
- номер полиса;
- описание снимка;
- отделение;
- причина смерти;
- причина снятия с учета;
- сведения из обращений;
- сведения о лечених;
- сведения о назначении лекарственных препаратов;
- сведения об обследовании;
- снимок;
- иные сведения, необходимые в соответствии с законодательством в сфере здравоохранения.

3.1.2 Законные представители/близкие родственники граждан, обратившихся за медицинской помощью:

- ФИО;
- дата рождения;
- адрес проживания;
- контактные телефоны;
- место работы;
- степень родства;
- сведения о состоянии здоровья;
- группа крови, резус принадлежность;
- данные флюорографических исследований.

Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается (ч. 4 ст. 13 ФЗ № 323-ФЗ):

- если пациент в результате своего состояния не способен выразить свою волю, но ему необходимо лечение;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

- в случае оказания медицинской помощи несовершеннолетнему, а также несовершеннолетнему, не достигшему возраста, установленного ч. 2 ст.54 ФЗ № 323-ФЗ, для информирования одного из его родителей или иного законного представителя;

- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий.

3.2 Получение персональных данных пациента преимущественно осуществляется путем представления пациентом письменного согласия на обработку персональных данных, за исключением случаев прямо предусмотренных действующим законодательством РФ.

В случае смерти пациента согласие на обработку его персональных данных дают в письменной форме наследники пациента, если такое согласие не было дано пациентом при его жизни.

3.3 Пациент, как субъект персональных данных, в том числе специальной категории персональных данных, имеет право на получение сведений:

- об операторе, о месте нахождения оператора;
- о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных;
- на подтверждение факта обработки персональных данных оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

3.4 Пациент имеет право:

- требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- доступа к своим персональным данным при личном обращении к представителю оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

3.5 При приеме к врачу пациент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- страховой полис обязательного медицинского страхования;
- в отдельных случаях с учетом специфики обследования в учреждение здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

4 Сбор, обработка и хранение персональных данных

4.1 Все персональные данные пациента следует получать у него самого. Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения медицинских карт для пациентов, которые хранятся в личном деле в регистратуре/архиве. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

4.2 Учреждение не имеет права получать и обрабатывать персональные данные пациента о его политических взглядах, религиозных или философских убеждениях.

4.3 Обработка персональных данных должна осуществляться на основе принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3 Согласие субъекта персональных данных не требуется в случаях, определенных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11, в том числе:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия Учреждения;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

В остальных случаях при обработке персональных данных необходимо руководствоваться ст. 6, 9-11 Федерального закона от 27 июля 2006 № 152-ФЗ.

4.4 Письменное согласие пациента на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Учреждения, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись.

4.5 Запрещается требовать от пациента, нуждающегося в оказании медицинской помощи, иные документы и/или персональные данные помимо предусмотренных Федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации в этой области.

4.6 Персональные данные субъектов хранятся в электронных базах данных и на бумажных носителях в регистратуре. Для этого используются специально оборудованные шкафы и сейфы. Личные дела пациентов (прошедших обследование, лечение) хранятся в архиве (хозяйственно-расчетном отделении) Учреждения.

4.7 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные телефоны и адрес электронной почты.

4.8 Персональные данные пациентов хранятся в электронных базах данных, которые могут быть подключены к локальной сети организации, а так же на бумажных носителях.

4.9 Доступ к электронным базам данных ограничен паролем. Возможна передача персональных данных пациентов между структурными подразделениями с использованием учтенных съемных носителей или по внутренней сети Учреждения с использованием технических и программных средств защиты информации, с доступом только для работников Учреждения, допущенных к работе с персональными данными пациентов Приказом Главного врача и только в объеме,

необходимом данным работникам для выполнения ими своих должностных обязанностей.

4.10 Обработка персональных данных без использования средств автоматизации (на бумажных носителях) осуществляется в соответствии с документом «Регламент обработки персональных данных без использования средств автоматизации в ГБУЗ СОКПБ. Неавтоматизированная обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие возможность несанкционированного доступа.

4.11 Бумажными носителями персональных данных являются:

- медицинская карта амбулаторного больного, которая заводится на каждого обратившегося в Учреждение за оказанием медицинской помощи при первом обращении и хранится в регистратуре Учреждения. Медицинская карта передается врачам-специалистам Учреждения при личном обращении пациента в Учреждение, по окончании приема медицинская карта сдается медсестрой врача-специалиста в регистратуру Учреждения;

- медицинская карта стационарного больного, которая заводится на каждого поступившего в стационар на лечение пациента в приемном отделении стационара Учреждения и хранится в течение всего срока пребывания пациента в стационаре в папке лечащего врача. В случае необходимости предоставления медицинской карты в другие подразделения Учреждения для проведения по назначению лечащего врача диагностических исследований, консультаций врачей-специалистов медицинская карта до начала исследования/консультации передается постовой медсестрой отделения медицинскому персоналу соответствующего подразделения, после проведения исследований/консультаций возвращается медицинским персоналом данного подразделения лечащему врачу;

- медицинская карта больного дневного стационара при больничном учреждении, дневного стационара при амбулаторно-поликлиническом учреждении, стационара на дому.

- журналы и другие формы медицинской документации, содержащие персональные данные пациентов, оформляются и хранятся в регистратуре, кабинетах врачей Учреждения в соответствии с требованиями действующих приказов.

- прочие документы, используемые при оказании медицинской помощи и содержащие персональные данные пациентов (акты, направления, договоры, квитанции и пр.), после оформления передаются работнику, допущенному к работе с

персональными данными, в должностные обязанности которого входит обработка этих данных.

Хранение окончанных производством документов, содержащих персональные данные пациентов, осуществляется в архиве (регистратуре) Учреждения.

Порядок учета машинных (электронных) носителей ПДн определен в документе «Регламент обращения с машинными носителями персональных данных в ГБУЗ СОКПБ».

4.12 Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению 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.

4.13 При получении сведений, составляющих персональные данные субъектов заинтересованные лица, имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

4.14 Сроки обработки персональных данных определяются в соответствии со сроком, указанным в согласии субъекта персональных данных, приказом Министерства культуры РФ от 25.08.2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями законодательства РФ и локальными актами Оператора.

4.15 Оператором создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию Оператором данных типовых форм документов установлены постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5 Передача персональных данных субъектов ПД

5.1 При передаче персональных данных субъектов работники Учреждения, имеющие доступ к персональным данным, должны соблюдать следующие требования:

5.1.1 Не сообщать персональные данные пациента третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах

охраны здоровья граждан в Российской Федерации» или иными федеральными законами.

5.1.2 Не сообщать персональные данные пациента в коммерческих целях без его письменного согласия.

5.1.3 Предупредить лиц, получающих персональные данные пациента, 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.

5.1.4 Разрешать доступ к персональным данным пациента только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

5.1.5 Все сведения о передаче персональных данных пациента должны регистрироваться в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившим запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана.

6 Защита персональных данных

6.1 Защита персональных данных в Учреждении представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

6.2 В целях обеспечения безопасности персональных данных при их обработке в информационных системах Учреждения:

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

- обеспечивать пропускной режим в соответствии с утвержденными документами по охране и осуществлению пропускного режима;

- помещения, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- доступ к информации в электронном виде должен осуществляться с использованием парольной защиты, а в информационных системах персональных данных - с использованием средств автоматизации в соответствии с нормативными документами;

- машинные (электронные) носители информации, содержащие персональные данные, учитывают в журнале учета носителей персональных данных.

6.3 Обеспечение безопасности персональных данных в информационных системах персональных данных осуществляется в соответствии с требованиями ст. 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119, нормативными и руководящими документами уполномоченных федеральных органов исполнительной власти.

6.4 Мероприятия по обеспечению безопасности персональных данных проводятся в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационным и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; приказом от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. №378 г. Москва "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

6.5 Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых Учреждением угроз безопасности персональных данных (модели угроз) и в зависимости от уровня защищенности информационной системы, определенного в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом ФСТЭК России от 1 ноября 2012 г. №1119.

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

6.7 Обеспечение безопасности персональных данных в информационных системах персональных данных без использования средств автоматизации осуществляется в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

6.8 Работники Учреждения, имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

7 Заключительные положения

7.1 Настоящее Положение является внутренним документом Учреждения, подлежащим размещению на официальном сайте оператора.

7.2 Настоящее Положение подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

7.3 Учреждение имеет право вносить изменения в настоящее Положение. При внесении изменений в заголовке Положения указывается дата последнего обновления редакции. Новая редакция Положения вступает в силу с момента ее размещения на Сайте, если иное не предусмотрено новой редакцией Положения.

7.4 К настоящему Положению и отношениям между Учреждением и субъектом персональных данных подлежит применению право Российской Федерации.

7.5 Контроль исполнения требований настоящего Положения осуществляется лицом, ответственным за обеспечение безопасности персональных данных Учреждения.

7.6 Ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.

8 Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

8.1 Дисциплинарная ответственность

Согласно статье 24 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований Федерального

закона, несут предусмотренную законодательством Российской Федерации ответственность.

Согласно статье 90 ТК РФ, лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Статьей 81 ТК РФ предусмотрено расторжение трудового договора в случае разглашения работником персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей

Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 40 ТК РФ и Правилами внутреннего трудового распорядка Общества.

8.2 Административная ответственность

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) могут привлекаться как Общество, так и конкретные работники, исполняющие соответствующие трудовые функции.

Лица, виновные в нарушении правил обработки ПДн, могут привлекаться к административной ответственности по следующим основаниям:

Статья КоАП РФ	Вид нарушения	Субъект нарушения	Ответственность
ст. 14.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	На граждан	Предупреждение или наложение штрафа в размере от 400 до 600 рублей
		На юридических лиц	Штраф в размере от 6000 до 10000 рублей.
ч. 6 ст. 14.12	Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными	На граждан	Штраф в размере от 600 до 1000 рублей
		На юридических лиц	Штраф в размере от 10000 до 16000 рублей

	нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 6 ст. 14.12 КоАП		
ст. 14.14	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.44 КоАП	На юридических лиц	Штраф в размере от 4000 до 6000 рублей
ч. 1 ст. 19.4	Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль), муниципальный контроль	На юридических лиц	Штраф в размере от 2000 до 4000 рублей
ч. 1 ст. 19.6	Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный контроль, об устранении нарушений законодательства	На граждан	Штраф в размере от 400 до 600 рублей
		На юридических лиц	Штраф в размере от 10000 до 20000 рублей
ст. 19.7	Непредставление или несвоевременное представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление в государственный орган (должностному лицу), орган	На граждан	Штраф в размере от 100 до 400 рублей
		На юридических лиц	Штраф в размере от 4000 до 6000 рублей

	<p>(должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, таких сведений (информации) в неполном объеме или в искаженном виде</p>		
--	---	--	--

**8.3. Уголовная ответственность за нарушение правил работы с ПДн
может наступить в следующих случаях**

Статья УК РФ	Вид нарушения	Ответственность
<p>ч. 1 ст. 147</p>	<p>Незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации</p>	<p>Штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода, осужденного за период до 18 месяцев, либо обязательными работами на срок до 460 часов, либо исправительными работами на срок до 1 года, либо принудительными работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 4 лет или без такового, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 4 лет</p>

<p>ч. 2 ст. 147</p>	<p>Незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, совершенные лицом с использованием своего служебного положения</p>	<p>Штраф в размере от 100 000 до 400 000 рублей или в размере заработной платы или иного дохода осужденного за периодот 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностьюна срок от 2 до 6 лет, либо принудительными работами на срок до 4лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должностиили заниматься определенной деятельностью на срок до 6 лет</p>
<p>ч. 4 ст. 147</p>	<p>Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно- телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия</p>	<p>Штраф в размере от 160 000 до 460 000 рублей или в размере заработной платы или иного дохода осужденного за периодот 18 месяцев до 4 лет, либо лишением права занимать определенные должностиили заниматься определенной деятельностью на срок от 4 до 6 лет, либо принудительными работами на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 6 лет с лишением права занимать определенные должностиили заниматься определенной деятельностью на срок до 6 лет</p>
<p>ч. 1 ст. 272</p>	<p>Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации</p>	<p>Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода, осужденного за период до 18месяцев, либо исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срокдо 2 лет, либо лишением свободы на тот же срок</p>

ч. 2 ст. 272	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или совершенное из корыстной заинтересованности	Штраф в размере от 100 000 до 400 000 рублей или в размере заработной платы или иного дохода осужденного за периодот 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок
ч. 4 ст. 272	Деяния, предусмотренные ч.1-2 ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения	Штраф в размере до 600 000 рублей или в размере заработной платы или иного дохода осужденного за период до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 4 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 6 лет, либо лишением свободы на тот же срок
ч. 4 ст. 272	Деяния, предусмотренные ч. 1-4 ст. 272 УК РФ, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ч. 1 ст. 274	Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 4 лет, либо лишение свободы на тот же срок со штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев
ч. 2 ст. 274	Деяния, предусмотренные ч. 1 ст. 274, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 4 лет или без такового, либо лишением свободы на срок до 6 лет со штрафом в размере от 100 000 до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2 до 4 лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 4 лет или без такового

ч. 4 ст. 274	Деяния, ч. 1-2 ст. 274, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ч. 1 ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончательного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб	Штраф в размере до 600 000 рублей или в размере заработной платы или иного дохода, осужденного за период до 18 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок
ч. 2 ст. 274	Деяние, предусмотренное ч.1 ст. 274, если оно повлекло тяжкие последствия или создало угрозу их наступления	Принудительные работы на срок до 6 лет либо лишением свободы на тот же срок

8.4 Гражданско-правовая ответственность

Порядок защиты нематериальных благ, к числу которых относятся честь и доброе имя, деловая репутация; неприкосновенность частной жизни; личная и семейная тайна определяется Гражданским кодексом РФ и иными законами.

