

**Положение
об обработке и обеспечении безопасности персональных данных
в ГАУЗ СО «ОНБ»**

Содержание

1. Назначение и область применения	3
2. Нормативные ссылки	3
3. Термины, их определения и сокращения	4
4. Принципы обработки ПДн	5
5. Цели и состав обрабатываемых ПДн.....	6
6. Назначение ответственного за организацию обработки ПДн	6
7. Порядок обработки ПДн	7
8. Условия обработки ПДн, осуществляемой без использования средств автоматизации	11
9. Порядок обеспечения безопасности ПДн	12
10. Взаимодействие с государственными органами (регуляторами).....	14
11. Ответственность	14
12. Порядок пересмотра (актуализации) Положения	15

1. Назначение и область применения

1.1. Положение об обработке и обеспечении безопасности персональных данных в ГАУЗ СО «ОНБ» (далее – Положение) устанавливает требования по организации и непосредственному функционированию процессов обработки и обеспечения безопасности персональных данных (далее – ПДн) в ГАУЗ СО «ОНБ» (далее – Учреждения) в соответствии с требованиями законодательства РФ в области обработки и защиты ПДн.

1.2. Положение определяет порядок обработки ПДн работников Учреждения и иных субъектов ПДн, данные которых подлежат обработке на основании полномочий Учреждения, порядок обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, а также устанавливает ответственность должностных лиц, имеющих доступ к ПДн, за невыполнение требований, регулирующих обработку и защиту ПДн.

1.3. Положение подлежит применению должностными лицами Учреждения, принимающими участие в процессах обработки и обеспечения безопасности ПДн.

2. Нормативные ссылки

2.1. В настоящем Положении использованы нормативные ссылки на следующие документы:

- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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»;
- Федеральный закон от 26.12.2008 № 294-ФЗ (ред. от 08.03.2022) «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;
- Регламент проведения аудитов информационной безопасности в ГАУЗ СО «ОНБ»;
- Порядок обработки обращений субъектов персональных данных в ГАУЗ СО «ОНБ»;

- Перечень персональных данных ГАУЗ СО «ОНБ»;
- Перечень должностей работников, допущенных к обработке персональных данных в ГАУЗ СО «ОНБ».

3. Термины, их определения и сокращения

3.1.В настоящем Положении применены следующие термины:

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);

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 Учреждением или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта персональных данных или иного законного основания;

несанкционированный доступ к персональным данным (несанкционированные действия): доступ к персональным данным или действия с персональными данными, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

обезличивание персональных данных: действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

оператор (персональных данных): ГАУЗ СО «ОНБ», самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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;

субъект персональных данных: физическое лицо, к которому относятся соответствующие персональные данные;

трансграничная передача персональных данных: передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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;

3.2. В настоящем Положении применены следующие условные обозначения:

ИСПДн – информационная система персональных данных;

ИВС – информационная вычислительная сеть;

Учреждение – ГАУЗ СО «ОНБ»;

ПДн – персональные данные;

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

РФ – Российская Федерация;

СЗПДн – система защиты персональных данных;

ФЗ-152 – Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

ФСБ России – Федеральная служба безопасности Российской Федерации;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации.

4. Принципы обработки ПДн

4.1. Обработка ПДн в Учреждении осуществляется на основании принципов:

– законности целей и способов обработки ПДн и добросовестности;

– соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения, а именно: содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников, контроль количества, качества выполняемой работы и обеспечение сохранности имущества и оказание медицинских услуг, в соответствии с договором с пациентом и законодательством РФ;

– соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

– достоверности и актуальности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

–недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных (далее – ИСПДн).

4.2.Хранение ПДн в Учреждении осуществляться исключительно в электронной форме, позволяющей определить субъекта ПДн. Обрабатываемые ПДн в бумажном виде подлежат немедленному уничтожению по достижении целей обработки.

5. Цели и состав обрабатываемых ПДн

5.1.Обработка ПДн осуществляется Учреждением для достижения конкретных и законных целей. Исходя из заданных целей обработки ПДн определяется состав ПДн, подлежащих обработке.

5.2.Перечень категорий субъектов ПДн, данные которых обрабатываются в Учреждении, состав ПДн, цели и правовые основания обработки для каждой из категорий субъектов ПДн, а также документы, устанавливающие сроки хранения документов, содержащих ПДн, документируются в «Перечне персональных данных ГАУЗ СО «ОНБ».

5.3.В Учреждении осуществляется обработка специальных категорий ПДн в случаях, предусмотренных законодательством РФ и с письменного согласия субъекта ПДн на обработку его ПДн.

5.4.В Учреждении осуществляется обработка ПДн в целях оказания медицинских услуг населению путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи только при условии получения предварительного согласия субъекта ПДн.

5.5.В Учреждении не осуществляется:

- обработка биометрических ПДн;
- трансграничная передача ПДн;
- принятие решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки ПДн.

5.6.Исходя из состава, целей и способов обработки ПДн, структуры информационной вычислительной сети (далее – ИВС) Учреждения, потоков информации и используемых информационных систем для обработки ПДн в Учреждении выделяются ИСПДн.

6. Назначение ответственного за организацию обработки ПДн

6.1.Для координации процессов обработки ПДн в Учреждении назначается работник, ответственный за организацию обработки ПДн (далее – Ответственный за организацию обработки ПДн).

6.2.Ответственный за организацию обработки ПДн:

- осуществляет внутренний контроль за соблюдением в Учреждении требований законодательства РФ о ПДн, в том числе требований к защите ПДн;
- доводит до сведения работников Учреждения положения законодательства РФ о ПДн, локальных актов Учреждения по вопросам обработки ПДн, требований к защите ПДн;

–организует и осуществляет контроль за приемом и обработкой обращений и запросов субъектов ПДн или их представителей в соответствии с «Регламентом обработки обращений субъектов ПДн в ГАУЗ СО «ОНБ».

7. Порядок обработки ПДн

7.1.Обработка ПДн в Учреждении осуществляется как с использованием средств автоматизации, так и без использования таких средств и действующим законодательством.

7.2.Способы обработки ПДн в Учреждении включают: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступа), блокирование, обезличивание, удаление, уничтожение ПДн.

7.3.Сбор ПДн

7.3.1. Сбор ПДн в Учреждении осуществляется только при наличии правового обоснования их обработки.

7.3.2. В Учреждении ПДн поступают из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ;
- от другого субъекта ПДн.

7.3.3. Сбор ПДн не от субъекта ПДн осуществляется только при соблюдении по меньшей мере одного из следующих условий:

–ПДн будут обрабатываться на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

–ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

–субъект ПДн уведомлен соответствующим оператором о передаче его ПДн в Учреждение и о целях получения его ПДн Учреждением, от субъекта ПДн получено письменное согласие и подписанная обеими сторонами доверенность на лицо, передающее ПДн субъекта в Учреждение;

7.3.4. При сборе ПДн до или в момент их получения в установленных случаях необходимо осуществлять сбор согласий на обработку ПДн. Ответственность за сбор и хранение согласий возлагается на работников Учреждения, осуществляющих сбор ПДн субъектов ПДн. Хранение согласий субъектов ПДн осуществляется в бумажном и (или) электронном виде.

7.3.5. Обработка ПДн в Учреждении осуществляется без получения согласий на обработку ПДн в следующих случаях:

–обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

–обработка ПДн необходима для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а

также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

–обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн;

–осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн, либо по его просьбе;

–осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством РФ.

7.3.6. Учреждение, в случае подписания трудового договора с субъектом ПДн не имеет права получать и обрабатывать данные о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья. ПДн субъекта подобного характера работодатель вправе обрабатывать только с письменного согласия субъекта.

7.4.Запись, систематизация и накопление ПДн

7.4.1. Ввод ПДн в ИСПДн осуществляется работниками Учреждения, имеющими доступ к работе с ПДн в соответствии с должностными обязанностями, или же субъектом ПДн самостоятельно при заполнении регистрационных форм на веб-сайте Учреждения.

7.4.2. Работники, осуществляющие ввод и обработку ПДн, несут ответственность за точность, достаточность, а в необходимых случаях и актуальность ПДн.

7.4.3. Запрещается демонстрация экранных форм, содержащих ПДн, лицам, не имеющим права доступа к соответствующим ПДн.

7.5.Хранение персональных данных

7.5.1. Бумажные и съемные портативные носители ПДн (USB-флэш-накопители, CD/DVD-диски) хранятся в шкафах или ящиках, запираемых на ключ без возможности получения доступа к таким носителям со стороны лиц, которым такой доступ не предоставлен.

7.5.2. Носители ПДн убираются в шкаф или ящик, запираемые на ключ, когда с носителем не ведется работа, а также покидая рабочее место, в том числе по окончании рабочего дня.

7.5.3. Запрещается копирование ПДн на несанкционированные съемные портативные носители информации. Все портативные носители информации, на которые осуществляется копирование ПДн, должны быть учтены в Журнале учета защищаемых электронных носителей.

7.6.Актуализация, уточнение, исправление, извлечение и использование ПДн

7.6.1. При использовании ПДн допускается:

–извлечение ПДн из баз данных или иных электронных хранилищ данных;

–формирование документов (как в электронном виде, так и на бумажных носителях), содержащих ПДн, в случаях, предусмотренных процессами обработки ПДн;

–передача таких документов как внутри Учреждения между работниками, в том числе различных структурных подразделений, так и третьим лицам в случаях, предусмотренных процессами обработки ПДн.

7.6.2. Субъект ПДн обязан предоставлять Учреждению достоверные сведения о себе и своевременно сообщать об изменении своих ПДн.

7.6.3. Работники Учреждения обязаны уточнять обрабатываемые ПДн и вносить в них необходимые изменения (при выявлении неполных или неточных ПДн субъекта ПДн) по требованию субъекта ПДн, его законного представителя или уполномоченного органа по защите прав субъектов ПДн (далее - Роскомнадзор) в соответствии с Регламентом обработки обращений субъектов ПДн.

7.6.4. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- сроки обработки ПДн, в том числе сроки их хранения;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или основании федерального закона;

7.6.5. Работники Учреждения обязаны уведомлять субъекта ПДн или его представителя о внесенных изменениях и принимать разумные меры для уведомления третьих лиц, которым ПДн этого субъекта ПДн были переданы.

7.7.Передача ПДн

7.7.1. Передача ПДн в пределах Учреждения

7.7.1.1.Передача ПДн в пределах Учреждения осуществляется посредством использования ИВС – размещения ПДн в информационных системах, сетевых папках, передачи по корпоративной электронной почте, в системе безбумажного документооборота и т.п., а также с использованием бумажных носителей ПДн. Передачу ПДн с использованием съемных машинных носителей разрешается осуществлять только в случае невозможности использования ИВС.

7.7.1.2.Допускается осуществлять передачу ПДн только работникам, имеющим доступ к соответствующим ПДн в объеме, который необходим для выполнения конкретных функций.

7.7.1.3.Руководители структурных подразделений Учреждения имеют доступ к ПДн работников соответствующих структурных подразделений в порядке административной и функциональной подчиненности.

7.7.1.4.Все работники Учреждения имеют доступ к корпоративному справочнику Учреждения.

7.7.2. Передача ПДн за пределы Учреждения

7.7.2.1.Учреждение в ходе своей деятельности осуществляет предоставление доступа (в т. ч. передачу) к ПДн третьим лицам в целях исполнения договорных обязательств перед субъектами ПДн, а также с целью обеспечения своей деятельности и исполнения требований нормативных документов РФ. При этом субъект ПДн может беспрепятственно получить доступ к перечню третьих сторон,

которым предоставляется доступ к его ПДн, если это не противоречит требованиям законодательства РФ.

7.7.2.2. Предоставление Учреждением доступа к ПДн субъекта ПДн третьим лицам осуществляется только при соблюдении следующих условий:

- передача ПДн осуществляется с согласия субъекта ПДн и/или при наличии правовых оснований, предусмотренных законодательством РФ;
- передача ПДн осуществляется с согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, или же исполнения договора, стороной которого, выгодоприобретателем, поручителем является субъект ПДн, а также случаях, предусмотренных Трудовым кодексом РФ и иными Федеральными законами РФ;
- передача ПДн осуществляется только в объеме, необходимом для достижения заявленных целей обработки ПДн;
- если передача обусловлена наличием договорных отношений, существенным условием договора с третьей стороной, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7.7.2.3. Если Учреждение поручает обработку ПДн третьим лицам с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, договор или его обязательные приложения должны устанавливать:

- обязанность лица, осуществляющего обработку ПДн по поручению Учреждения, по соблюдению принципов и правил обработки ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн по поручению Учреждения;
- цели обработки ПДн;
- обязанность лица, осуществляющего обработку ПДн по поручению Учреждения, по соблюдению конфиденциальности ПДн и обеспечению безопасности ПДн;
- требования по обеспечению безопасности ПДн, которые должны быть выполнены лицом, осуществляющим обработку ПДн по поручению Учреждения.

7.7.2.4. В порядке, установленном законодательством РФ, ПДн отдельных субъектов ПДн могут быть предоставлены их законным представителям, государственным органам и/или органам местного самоуправления.

7.7.2.5. Ответственность за соблюдение порядка предоставления ПДн субъекта ПДн третьим лицам несет работник Учреждения, а также руководитель структурного подразделения, осуществляющего передачу ПДн субъекта ПДн третьему лицу.

7.8. Блокирование ПДн

7.8.1. Учреждение блокирует обрабатываемые ПДн при выявлении их недостоверности или неправомерных действий в отношении субъекта ПДн по требованию субъекта ПДн, его законного представителя или Роскомнадзора в соответствии с Регламентом обработки обращений субъектов ПДн или по

результатам внутренних контрольных мероприятий, осуществляемых в соответствии с Регламентом проведения аудитов информационной безопасности в ГАУЗ СО «ОНБ».

7.9.Обезличивание, удаление и уничтожение ПДн

7.9.1. Учреждение уничтожает ПДн в случае:

- достижения целей обработки ПДн или утраты необходимости в их достижении;
- отзыва согласия субъекта ПДн на обработку его ПДн, если отзыв согласия влечет за собой уничтожение ПДн;
- получения соответствующего предписания от Роскомнадзора.

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

7.9.3. Ответственность за своевременное уничтожение носителей ПДн, находящихся в оперативном хранении, возлагается на работников, допущенных к обработке ПДн, а контроль за исполнением этого требования – на соответствующих руководителей структурных подразделений.

7.9.4. Уничтожение носителей ПДн, находящихся на архивном хранении, осуществляется в установленном в Учреждении порядке.

8. Условия обработки ПДн, осуществляемой без использования средств автоматизации

8.1.При неавтоматизированной обработке ПДн должны обособляться от иной информации путем фиксации на отдельных материальных носителях либо в специальных разделах или полях форм и бланков, которые могут содержать ПДн.

8.2.Не допускается фиксация на одном материальном носителе данных, цели обработки которых заведомо не совместимы. Для ПДн, обрабатываемых с различными целями, должны использоваться различные материальные носители, хранящиеся отдельно друг от друга.

8.3.В Учреждении используются формы документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы).

8.4.При использовании типовых форм должны соблюдаться следующие условия:

- в типовые формы или в связанные с ними документы (инструкция по ее заполнению, карточки, реестры и журналы) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Учреждения, Ф.И.О. и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Учреждении способов обработки ПДн;

- в случае необходимости получения письменного согласия на обработку ПДн, в типовую форму включается поле, в котором субъект ПДн может поставить

отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;

– типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, чьи ПДн содержатся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

– в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

8.5. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными ПДн.

8.6. Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей).

9. Порядок обеспечения безопасности ПДн

9.1. С целью выполнения требований законодательства РФ в области ПДн, Учреждение считает важнейшей задачей обеспечение конфиденциальности, целостности и доступности ПДн при их обработке. Для решения данной задачи в Учреждении введена, функционирует и проходит периодический пересмотр (контроль) система защиты ПДн.

9.2. В Учреждении принимаются необходимые правовые, организационные и технические меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, от иных неправомерных действий в отношении ПДн.

Процесс обеспечения безопасности ПДн в Учреждении является непрерывным и постоянно поддерживается работниками Учреждения, осуществляющими обработку и обеспечение безопасности ПДн в Учреждении.

9.3. Для координации процессов обеспечения безопасности ПДн в Учреждении назначается работник, ответственный за обеспечение безопасности ПДн (далее – Ответственный за обеспечение безопасности ПДн).

9.4. Мероприятия по обеспечению безопасности ПДн

9.4.1. Обеспечение безопасности ПДн при их обработке в Учреждении осуществляется выполнением следующих мероприятий:

– определение угроз безопасности ПДн при их обработке в ИСПДн;

– применение необходимых программных и программно-аппаратных средств защиты, в частности средств защиты от несанкционированного доступа, средств разграничения доступа и регистрации действий пользователей, средств антивирусной защиты, анализа защищенности, обнаружения вторжений, резервного копирования, межсетевых экранов при взаимодействии с сетью Интернет и др.;

– ограничение доступа в помещения, в которых размещены технические средства обработки ПДн, а также носители информации, содержащие ПДн;

- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета действий, совершаемых с ПДн в ИСПДн;
- определение перечня лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей;
- учет и хранение носителей информации содержащих ПДн, их обращение, исключающее хищение, подмену и уничтожение;
- обнаружение фактов несанкционированного доступа к ПДн и принятием мер;
- резервирование технических средств, дублирование массивов и носителей, содержащих ПДн;
- использование защищенных каналов связи для передачи ПДн;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- регистрация событий и мониторинг процессов обработки ПДн;
- использование средств антивирусной защиты;
- контроль эффективности применяемых мер и средств по обеспечению безопасности ПДн, а также контролем уровня защищенности ИСПДн;
- оценка вреда, который может быть причинен субъектам ПДн.

9.4.2. Доступ работникам Учреждения к ПДн, в том числе к ИС, в которых обрабатывается ПДн, предоставляется, если такой доступ необходим ему для выполнения служебных (трудовых) обязанностей. Для определения перечня указанных работников разрабатывается и утверждается «Перечне должностей работников, допущенных к обработке персональных данных в ГАУЗ СО «ОНБ», в котором указываются структурные подразделения, должности, отдельные лица (при необходимости) и группы ПДн, к работе с которыми они допущены.

9.4.3. Все используемые в процессах обработки ПДн Учреждения носители подлежат учету. Учет съемных портативных носителей информации осуществляется в соответствии с п 7.5.3. Учет жестких дисков осуществляется совместно с техническими средствами, в которых они установлены должностными лицами, ответственными за сопровождение ИВС Учреждения.

9.4.4. В случаях, предусмотренных законодательством РФ, в рамках системы защиты ПДн применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия.

9.5.Проведение контрольных мероприятий по обеспечению безопасности ПДн

9.5.1. Проведение контрольных мероприятий по обеспечению безопасности ПДн осуществляется с целью приведения существующей СЗПДн в соответствие с текущими процессами обработки ПДн, структурой ИВС Учреждения, требованиями организационно-распорядительных документов Учреждения и законодательства РФ.

9.5.2. Контрольные мероприятия проводятся в рамках общекорпоративных мероприятий в соответствии с Регламентом проведения аудитов информационной безопасности в ГАУЗ СО «ОНБ» и должны включать:

–оценку соответствия процессов обработки и обеспечения безопасности ПДн требованиям организационно-распорядительных документов Учреждения и законодательства РФ;

–оценку эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн.

9.5.3. Комплексные контрольные мероприятия по обеспечению безопасности ПДн должны проводиться не реже одного раза в три года.

9.5.4. По результатам проведения контрольных мероприятий должностными лицами Учреждения, ответственными за управление рисками ИБ и поддержание режима ИБ, должны планироваться и инициироваться мероприятия по устранению выявленных несоответствий и совершенствованию СЗПДн.

10. Взаимодействие с государственными органами (регуляторами)

10.1. Уполномоченным органом по защите прав субъектов ПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки ПДн требованиям ФЗ-152, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

10.2. В соответствии с ФЗ-152 Учреждение осуществляет уведомление Роскомнадзора в следующих случаях:

–в случае изменения сведений, указанных в Уведомлении об обработке ПДн, поданном в Роскомнадзор перед началом обработки ПДн;

–по факту внесения Учреждением изменений в ПДн на основании запроса Роскомнадзора;

–по факту устранения выявленных нарушений, выполненных на основании правомерного запроса Роскомнадзора;

–по факту уничтожения ПДн, если на основании правомерного запроса Роскомнадзора обеспечить правомерность обработки ПДн Учреждением.

Формы уведомлений Роскомнадзора представлены в Приложениях А.1, А.2, А.3.

10.3. Федеральные органы исполнительной власти ФСБ России и ФСТЭК России решением Правительства РФ могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн.

10.4. Контроль и надзор за выполнением требований по обработке и обеспечению безопасности ПДн осуществляется Роскомнадзором и Федеральными органами исполнительной власти без права ознакомления с ПДн, обрабатываемыми в Учреждении, за исключением, когда ознакомление с ПДн осуществляется в соответствии с Федерального законодательства РФ.

11. Ответственность

11.1. Каждый работник, осуществляющий обработку ПДн, несет персональную ответственность за соблюдение требований настоящего Положения и обеспечение мер по защите ПДн на своем рабочем месте.

11.2. Учреждение, в случае нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных

правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

11.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной, гражданско-правовой, административной и иным видам ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

12. Порядок пересмотра (актуализации) Положения

12.1. Все изменения и дополнения, необходимые для внесения в текст настоящего Положения, производятся посредством выпуска организационно-распорядительного документа об изменении (не более двух) согласованного с кругом лиц, которых затрагивает вносимое изменение.

12.2. Пересмотр Положения осуществляется не реже, чем раз в 3 (три) года, после чего осуществляется утверждение организационно-распорядительным документом его новой редакции, либо продление срока действия.

12.3. Контроль над внесением изменений (пересмотром) настоящего Положения возлагается на разработчика.

А.1

Уведомление о внесении изменений в ПДн

Руководителю территориального
Управления Федеральной службы по
надзору в сфере связи, информационных
технологий и массовых коммуникаций
по Уральскому федеральному округу

УВЕДОМЛЕНИЕ о внесении изменений в персональные данные

Тип оператора: Юридическое лицо

Наименование: ГАУЗ СО «ОНБ»

Адрес: г. Екатеринбург, пр Ленина 7

руководствуясь:

_____ (правовое основание обработки персональных данных)

в отношении персональных данных:

_____ (имя субъекта персональных данных)

на основании:

_____ (основание внесения изменений в персональные данные)

внесло следующие изменения:

Состав персональных данных (ФИО, адрес, телефон и т.п.)	исходное значение	измененное значение

Указанные персональные данные вводятся в обработку с учетом внесенных изменений начиная с

_____ (дата возобновления обработки)

Срок или условие прекращения обработки персональных данных

_____ (должность)

_____ (подпись)

_____ (ФИО)

«__» _____ 202_ г.

А.2 Уведомление об уничтожении ПДн

Руководителю территориального Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому федеральному округу

УВЕДОМЛЕНИЕ об уничтожении персональных данных

Тип оператора: юридическое лицо

Наименование: ГАУЗ СО «ОНБ»

Адрес: г. Екатеринбург, пр. Ленина 7

руководствуясь:

_____ (правовое основание обработки персональных данных)

в целях:

_____ (цель обработки персональных данных)

осуществляло обработку следующего состава персональных данных:

_____ (перечень ПДн)

принадлежащих

_____ (имя субъекта персональных данных)

_____ (если имеются, дополнительные сведения для идентификации: дата рождения / адрес...)

с

по

_____ (дата начала обработки персональных данных)

_____ (дата прекращения обработки)

Обработка вышеуказанных персональных данных оператором была прекращена, а сами данные уничтожены в связи с:

_____ (причина прекращения обработки персональных данных: окончание срока обработки или событие, с которым связано достижение цели или утрата необходимости обработки)

_____ (должность)

_____ (подпись)

_____ (ФИО)

«__» _____ 202__ г.

А.3 Уведомление об устранении нарушений в порядке обработки ПДн

Руководителю территориального Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому федеральному округу

УВЕДОМЛЕНИЕ об устранении нарушений в порядке обработки персональных данных

Тип оператора: юридическое лицо

Наименование: ГАУЗ СО «ОНБ»

Адрес: г. Екатеринбург, пр Ленина 7

В отношении порядка обработки персональных данных, принадлежащих:

(имя субъекта персональных данных и дополнительные сведения для идентификации, если имеются: дата рождения / адрес...)

Были допущены следующие нарушения:

(указать выявленные нарушения)

Указанные нарушения были устранены

(дата устранения нарушений)

на основании:

(правовое основание устранения выявленных нарушений)

Персональные данные вновь вводятся в обработку с

(дата ввода в обработку)

Срок или условие прекращения обработки персональных данных:

(должность)

(подпись)

(ФИО)

«__» _____ 202__ г.

Лист регистрации изменений

№ п/п	Основание (дата, номер)	Номера листов (пунктов)			ФИО, подпись
		измененных	замененных	новых	

Лист ознакомления

№ п/п	ФИО сотрудника	Должность	Подразделение	Дата ознакомления	Примечание
1					
2					
3					
4					
5					