



Для целей настоящего Положения применяются следующие термины и определения:

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

**Оператор Персональных данных** – Государственное бюджетное учреждение здравоохранения «Центр реабилитации слуха» (далее Учреждение) – субъект, 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;

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

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа к информационным системам персональных данных** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия

решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

- **Блокирование персональных данных** –временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- **Обезличивание персональных данных** –действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту 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 оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
- Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.
- Обеспечения конфиденциальности персональных данных не требуется: 1) в случае обезличивания персональных данных; 2) в отношении общедоступных персональных данных.
- Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

### **Общедоступные источники персональных данных**

- В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).
- В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский

- номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
- Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

**Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Защита информации** – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

## 1. Общие положения

Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников Учреждения и граждан.

Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) 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 иные несанкционированные действия.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:

- предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов НСД к ПДн;
- постоянный контроль над обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн), в соответствии с утвержденными Требованиями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения (Приложение № 1).

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

- а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;
- г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;
- д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) учет лиц, допущенных к работе с ПДн в информационной системе;
- з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- к) описание системы защиты персональных данных.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской

Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

## **2. Цели обеспечения информационной безопасности**

Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации.

### 3. Объект защиты

Объектом защиты являются:

а) персональные данные работников Учреждения и граждан.

В целях ведения персонифицированного учета осуществляется обработка следующих персональных данных о лицах, которые участвуют в оказании медицинских услуг:

- 1) фамилия, имя, отчество (последнее - при наличии);
- 2) пол;
- 3) дата рождения;
- 4) место рождения;
- 5) гражданство;
- 6) данные документа, удостоверяющего личность;
- 7) место жительства;
- 8) место регистрации;
- 9) дата регистрации;
- 10) страховой номер индивидуального лицевого счета (при наличии),
- 11) сведения об образовании, в том числе данные об образовательных организациях и о документах об образовании и (или) о квалификации;
- 12) наименование организации, оказывающей медицинские услуги;
- 13) занимаемая должность в организации, оказывающей медицинские услуги.

В системе персонифицированного учета осуществляется обработка следующих персональных данных о лицах, которым оказываются медицинские услуги:

- 1) фамилия, имя, отчество (последнее - при наличии);
- 2) пол;
- 3) дата рождения;
- 4) место рождения;
- 5) гражданство;
- 6) данные документа, удостоверяющего личность;
- 7) место жительства;
- 8) место регистрации;
- 9) дата регистрации;
- 10) страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством РФ об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
- 11) номер полиса обязательного медицинского страхования застрахованного лица (при наличии);
- 12) анамнез;
- 13) диагноз;
- 14) сведения об организации, оказавшей медицинские услуги;
- 15) вид оказанной медицинской помощи;

- 16) условия оказания медицинской помощи;
- 17) сроки оказания медицинской помощи;
- 18) объем оказанной медицинской помощи;
- 19) результат обращения за медицинской помощью;
- 20) серия и номер выданного листка нетрудоспособности (при наличии);
- 21) сведения об оказанных медицинских услугах;
- 22) примененные стандарты медицинской помощи;
- 23) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу.

б) помещения объектов Учреждения, в которых размещаются информационные ресурсы и обрабатывается конфиденциальная информация;

в) технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Критичными свойствами объекта защиты являются:

а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

в) несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;
- прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);
- перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).



## 4. Субъекты информационных отношений

4.1 Субъектами информационных отношений являются:

- работники;
- граждане;

4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты персональных данных, защиты авторских прав, прав собственника информации).

## 5. Возможные угрозы и участки вторжения

Общая классификация угроз.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.

2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.

3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

4. Угрозы отказа от выполнения транзакций. Реализуются при создании условий легальному пользователю для отказа от выполненной операции по передаче или приему информации.

## **6. Порядок проведения контрольных мероприятий и действий по результатам контроля**

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Контроль может проводиться Комиссией, созданной в Учреждении, или на договорной основе сторонними организациями, при наличии лицензии на деятельность по технической защите конфиденциальной информации.

Решение основных вопросов обеспечения защиты ПДн предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения.

**СОГЛАСОВАНО**  
Юрисконсульт  
*А.В. Барина*  
А.В. Барина  
«    »    20    К.О.