

Приложение №1  
к приказу  
ГБУ РО «ГБ №1» в г. Волгодонске  
от 07.03.2023 № 172-А

**УТВЕРЖДАЮ:**  
Главный врач ГБУ РО «ГБ №1» в г. Волгодонске

07.03.2023г.  В.Ю. Бачинский



# **КОНЦЕПЦИЯ информационной безопасности информационных систем персональных данных в ГБУ РО «ГБ №1» в г. Волгодонске**

## 1. Определения

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**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.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**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 (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, 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.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## 2. Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

## 3. Введение

**3.1.** Настоящая Концепция информационной безопасности ИСПДн Государственного бюджетного учреждения Ростовской области "Городская больница №1" в г. Волгодонске (далее – ГБУ РО "ГБ №1" в г. Волгодонске) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности ГБУ РО "ГБ №1" в г. Волгодонске.

**3.2.** Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов при обработке информации вообще, и персональных данных в частности.

**3.3.** Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) ГБУ РО "ГБ №1" в г. Волгодонске. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

**3.4.** Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

**3.5.** Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

**3.6.** Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ГБУ РО "ГБ №1" в г. Волгодонске, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

3.7. Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности структурных подразделений ГБУ РО "ГБ №1" в г. Волгодонске при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске.

3.8. Область применения Концепции распространяется на все структурные подразделения ГБУ РО "ГБ №1" в г. Волгодонске, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

3.9. Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

#### 4. Общие положения

4.1. СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

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

4.3. 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.

4.4. Эти меры призваны обеспечить:

- **конфиденциальность** информации (защита от несанкционированного ознакомления);
- **целостность** информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

4.5. Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

4.6. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

#### 5. Задачи СЗПДн

5.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

5.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;
- аппаратным, программным и криптографическим средствам защиты, используемым

в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

## **6. Объекты защиты**

**6.1.** В ГБУ РО "ГБ №1" в г. Волгодонске производится обработка персональных данных в информационной системе обработки персональных данных (ИСПДн).

### **6.2. Перечень объектов защиты.**

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, обрабатываемых в ГБУ РО "ГБ №1" в г. Волгодонске.

Объекты защиты включают:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

## **7. Классификация пользователей ИСПДн**

**7.1.** Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник ГБУ РО "ГБ №1" в г. Волгодонске, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

**7.2.** Пользователи ИСПДн делятся на три основные категории:

7.2.1. Администратор ИСПДн. Сотрудники ГБУ РО "ГБ №1" в г. Волгодонске, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

7.2.2. Администратор безопасности ИСПДн. Сотрудники ГБУ РО "ГБ №1" в г. Волгодонске или сторонних организаций, которые занимаются разработкой программного обеспечения. Администратор безопасности ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

7.2.3. Пользователь ИСПДн. Сотрудники подразделений ГБУ РО "ГБ №1" в г. Волгодонске участвующих в процессе эксплуатации ИСПДн. Пользователь ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

7.3. Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

7.4. Все выявленные группы пользователей отражаются в Перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в ГБУ РО "ГБ №1" в г. Волгодонске. На основании обследования определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих ГБУ РО "ГБ №1" в г. Волгодонске.

## **8. Основные принципы построения системы комплексной защиты информации**

8.1. Построение системы обеспечения безопасности ПДн ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

### **8.2. Законность.**



8.2.1. Предполагает осуществление защитных мероприятий и разработку СЗПДн ГБУ РО "ГБ №1" в г. Волгодонске в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

8.2.2. Пользователи и обслуживающий персонал ПДн ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

### **8.3. Системность.**

8.3.1. Системный подход к построению СЗПДн ГБУ РО "ГБ №1" в г. Волгодонске предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске.

8.3.2. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

### **8.4. Комплексность.**

8.4.1. Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

8.4.2. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

8.4.3. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

### **8.5. Непрерывность защиты ПДн.**

8.5.1. Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

8.5.2. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

8.5.3. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

### **8.6. Своевременность.**

8.6.1. Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

8.6.2. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

### **8.7. Преемственность и совершенствование.**

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа

функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

#### **8.8. Персональная ответственность.**

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

#### **8.9. Принцип минимизации полномочий.**

8.9.1. Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

8.9.2. Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

#### **8.10. Взаимодействие и сотрудничество.**

8.10.1. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

8.10.2. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

#### **8.11. Гибкость системы защиты ПДн.**

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

#### **8.12. Открытость алгоритмов и механизмов защиты.**

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

#### **8.13. Простота применения средств защиты.**

8.13.1. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных затрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

8.13.2. Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

#### **8.14. Научная обоснованность и техническая реализуемость.**

8.14.1. Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

8.14.2. СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

#### **8.15. Специализация и профессионализм.**

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами ГБУ РО "ГБ №1" в г. Волгодонске.

#### **8.16. Обязательность контроля.**

8.16.1. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

8.16.2. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## **9. Меры, методы и средства обеспечения требуемого уровня защищенности**

**9.1.** Обеспечение требуемого уровня защищенности должности достигается с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

### **9.2. Законодательные (правовые) меры защиты.**

9.2.1. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

9.2.2. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

### **9.3. Морально-этические меры защиты.**

9.3.1. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писанные, то есть оформленные в некоторый свод (устав) правил или предписаний.

9.3.2. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

### **9.4. Организационные (административные) меры защиты.**

9.4.1. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

9.4.2. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

9.4.3. Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

9.4.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;

- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне ГБУ РО "ГБ №1" в г. Волгодонске в целом;

- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

9.4.5. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

9.4.6. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;

- кто имеет права доступа к ПДн;

- какими мерами и средствами обеспечивается защита ПДн;

- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

9.4.7. Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

9.4.8. Организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;

- порядок допуска сотрудников к использованию ресурсов ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске;

- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

- инструкций пользователей ИСПДн (администратора ИСПДн, пользователя ИСПДн);

- инструкция пользователя при возникновении внештатных ситуаций.

## 9.5. Физические меры защиты.

9.5.1. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

9.5.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

## 9.6. Аппаратно-программные средства защиты ПДн.

9.6.1. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

9.6.2. С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн МУЗ "Городская больница №1";
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

9.6.3. Успешное применение технических средств защиты на основании принципов (раздел 8) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании приказов главного врача ГБУ РО "ГБ №1" в г. Волгодонске;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т.п.);
- специалистами ГБУ РО "ГБ №1" в г. Волгодонске осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## **10. Контроль эффективности системы защиты**

**10.1.** Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

**10.2.** Контроль может проводиться как администраторами ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

**10.3.** Контроль может осуществляться администратором ИСПДн как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

**10.4.** Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## **11. Сферы ответственности за безопасность ПДн**

**11.1.** Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является Ответственный за информационную безопасность.

**11.2.** Сфера ответственности учреждения включает следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- контроль защищенности ИТ инфраструктуры ГБУ РО "ГБ №1" в г. Волгодонске от угроз ИБ путем;
- обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

**11.3.** При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 6), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

## **12. Модель нарушителя безопасности**

**12.1.** Под нарушителем в ГБУ РО "ГБ №1" в г. Волгодонске понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 6).

**12.2.** Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

## **13. Модель угроз безопасности**

**13.1.** Для ИСПДн ГБУ РО "ГБ №1" в г. Волгодонске выделяются следующие основные категории угроз безопасности персональных данных:

13.1.1. Угрозы от утечки по техническим каналам.

13.1.2. Угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
- угрозы преднамеренных действий внутренних нарушителей;
- угрозы несанкционированного доступа по каналам связи;
- описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

## **14. Механизм реализации Концепции**

**14.1.** Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

## **15. Ожидаемый эффект от реализации Концепции**

**15.1.** Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;
- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

15.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

## 16. Список использованных источников

16.1. Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика, являются:

- Федеральный Закон от 27.07.2006г. №152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012г. №1119.
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008г. №687.
- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008г. №512 (с изменениями и дополнениями).

### СОГЛАСОВАНО:

Заместитель главного врача  
по мобилизационной работе и ГО



В.В. Крамаров

Юрисконсульт

Ю.Ю. Никифорова

Разработал: Специалист по защите информации



Ю.Э. Айрапетян