

УТВЕРЖДЕНО  
приказом директора МБУ «КЦСОН «Добрыня»  
« 27 » апреля 2023 г. № 11

**КОНЦЕПЦИЯ**  
**информационной безопасности информационных систем персональных данных**  
**в муниципальном бюджетном учреждении «Комплексный центр социального**  
**обслуживания населения «Добрыня»**

**1. Термины и определения**

В настоящей Концепции информационной безопасности информационных систем персональных данных в муниципальном бюджетном учреждении «Комплексный центр социального обслуживания населения «Добрыня» (далее - Концепция) 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 защищённости персональных данных, характеризующееся 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 её использования;

**закладочное устройство** - элемент средства съёма информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съёма 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** - 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-распределённое 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 извлечённых из такой системы, считается осуществлённой 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 персональных данных (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 её функционирования;

**правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

**программная закладка** - код программы, преднамеренно внесённый 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 определённому 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. Условные 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 защищённости;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных;

СОВ - система обнаружения вторжений;

СУБД - система управления базами данных;

ТКУИ - технические каналы утечки информации;

УБПДн - угрозы безопасности персональных данных.

## 3. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения СЗПДн ИСПДн, используемых в муниципальном бюджетном учреждении «Комплексный центр социального обслуживания населения «Добрыня» (далее - Учреждение). Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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.

Под информационной безопасностью ПДн понимается защищённость ПДн и

обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её 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.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Учреждения;

- принятия управленческих решений и разработки практических мер для реализации 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 Учреждения 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 Учреждения.

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.

Безопасность ПДн достигается путём исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн.

СЗПДн включает в себя 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.

СЗПДн призвана обеспечить:

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

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического задания на разработку системы обеспечения безопасности информационного объекта вычислительной техники Учреждения;

- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приёмосдаточные испытания средств защиты информации, а также оценку соответствия

ИСПДн требованиям безопасности информации.

Организационные меры как составная часть СЗПДн включают в себя создание и поддержание правовой базы безопасности ПДн, мероприятия по обеспечению защиты ПДн в ИСПДн, внутренних проверок режима защиты ПД в информационных системах персональных данных, порядка резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ в информационных системах персональных данных, разработка и введение в действие должностной инструкции администратора безопасности информации Учреждения в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Технические средства защиты информации реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер и средств защиты информации определяется по результатам внутренней проверки обеспечения защиты ПДн в ИСПДн Учреждения.

#### **4. Задачи системы защиты ПДн**

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

Для достижения основной цели СЗПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке 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 должностных обязанностей), то есть защиту от несанкционированного доступа:

- а) к информации, циркулирующей в ИСПДн;

- б) средствам вычислительной техники ИСПДн;

- в) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- контроль целостности (обеспечение неизменности) среды исполнения программ и её 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 их обработке, хранении и передаче по каналам связи;

- защиту ПДн, хранимых, обрабатываемых и передаваемых 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 неправомерными действиями физических и юридических лиц ущерба, ослабления негативного влияния и ликвидация последствий нарушения безопасности ПДн.

## **5. Объекты защиты**

### **5.1. Перечень ИСПДн**

В Учреждении производится обработка ПДн в ИСПДн.

Перечень ИСПДн определяется на основании результатов проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных Учреждения.

### **5.2. Перечень объектов защиты**

Объектами защиты являются - информация, обрабатываемая в ИСПДн, технические средства её обработки и защиты.

Перечень ПДн, подлежащих защите, определен в Политике в отношении обработки персональных данных в МБУ «КЦСОН «Добрыня».

Объекты защиты включают в себя:

- 1) обрабатываемую информацию;
- 2) технологическую информацию;
- 3) программно-технические средства обработки;
- 4) каналы информационного обмена;
- 5) помещения, в которых размещены компоненты ИСПДн.

## **6. Классификация пользователей ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционировании ИСПДн или использующее результаты её функционирования. Пользователем ИСПДн является любой работник Учреждения, имеющий доступ к ИСПДн и её ресурсам в соответствии с установленным порядком и его функциональными обязанностями.

Пользователи ИСПДн делятся на следующие основные категории:

1. Администратор безопасности ИСПДн (работник Учреждения или третьи лица, которые занимаются настройкой, внедрением и сопровождением ИСПДн). Администратор безопасности 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.

2. Пользователь ИСПДн (работники Учреждения, участвующие 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.

Все работники Учреждения имеют допуск в соответствии с занимаемой должностью к работе с ПДн, утвержденный приказом директора Учреждения.

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

Построение системы обеспечения безопасности ПДн ИСПДн Учреждения и её функционирование должны осуществляться в соответствии со следующими основными



принципами:

- 1) законность;
- 2) системность;
- 3) комплексность;
- 4) непрерывность;
- 5) своевременность;
- 6) преемственность и непрерывность совершенствования;
- 7) персональная ответственность;
- 8) минимизация полномочий;
- 9) взаимодействие и сотрудничество;
- 10) гибкость системы защиты;
- 11) открытость алгоритмов и механизмов защиты;
- 12) простота применения средств защиты;
- 13) научная обоснованность и техническая реализуемость;
- 14) специализация и профессионализм;
- 15) обязательность контроля.

### **7.1. Законность**

Предполагает осуществление защитных мероприятий и разработку СЗПДн Учреждения в соответствии с требованиями законодательства в области защиты ПДн и других нормативных актов по безопасности информации, утверждённых органами государственной власти в пределах их компетенции.

Пользователи и обслуживающий персонал ИСПДн Учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

### **7.2. Системность**

Системный подход к построению СЗПДн Учреждения предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Учреждения.

При создании СЗПДн 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 распределённые системы и НСД к информации. СЗПДн должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

### **7.3. Комплексность**

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

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

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства

криптографической защиты. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

#### **7.4. Непрерывность**

Защита ПДн – это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

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

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 её функционирования.

#### **7.5. Своевременность**

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 её системы защиты информации, в частности.

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

#### **7.6. Преемственность и непрерывность совершенствования**

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и её системы защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

#### **7.7. Персональная ответственность**

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

#### **7.8. Минимизация полномочий**

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

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

#### **7.9. Взаимодействие и сотрудничество**

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Учреждения, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке специалисты должны осознанно соблюдать установленные

правила и оказывать содействие в деятельности ответственного за функционирование ИСПДн.

#### **7.10. Гибкость системы защиты**

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 защищённости 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 её нормального функционирования.

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

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

#### **7.12. Простота применения средств защиты**

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 в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

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

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.

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

#### **7.14. 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 Учреждения.

#### **7.15. Обязательность контроля**

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.

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.

## **8. Меры, методы и средства обеспечения требуемого уровня защищённости**

Обеспечение требуемого уровня защищённости должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

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

### **8.1. Законодательные (правовые) меры обеспечения безопасности ИСПДн**

К законодательным (правовым) мерам обеспечения безопасности ИСПДн относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Законодательные (правовые) меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

### **8.2. Морально-этические меры обеспечения безопасности ИСПДн**

К морально-этическим мерам обеспечения безопасности ИСПДн 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 утверждённые нормативные акты, однако их несоблюдение ведёт 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.

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.

### **8.3. Организационные (административные) меры обеспечения безопасности ИСПДн**

Организационные (административные) меры обеспечения безопасности ИСПДн - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность администратора безопасности информации, 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.

Главная цель административных мер, предпринимаемых Учреждением - подход к защите информации, выделение необходимых ресурсов и контроля состояния дел.

К административному уровню относятся решения руководства Учреждения, затрагивающие деятельность ИСПДн в целом. Примером таких решений могут быть:

- формулирование целей, постановка задач, определение направлений деятельности в

области безопасности ПДн;

- обеспечение нормативной базы вопросов безопасности и т.п.

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 (аппаратными) 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.

Организационные меры должны состоять из:

- порядка допуска работников к использованию ресурсов ИСПДн Учреждения;
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
- инструкций администратора безопасности ИСПДн, пользователя (оператора) ИСПДн).

#### **8.4. Физические меры обеспечения безопасности ИСПДн**

Физические меры обеспечения безопасности ИСПДн 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.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём 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.

#### **8.5. Технические (аппаратно-программные) меры обеспечения безопасности ИСПДн**

Технические (аппаратно-программные) меры обеспечения безопасности ИСПДн 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.).

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

- средства защиты от несанкционированного доступа;
- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к

ресурсам ИСПДн Учреждения;

- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- средства защиты от утечки информации по техническим каналам связи и по каналам побочных электромагнитных излучений и наводок;
- криптографические и антивирусные средства защиты ПДн;
- программно-аппаратные средства защиты информации.

Успешное применение технических мер обеспечения безопасности ИСПДн на основании основных принципов построения системы комплексной защиты информации (раздел 7 настоящей Концепции) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонентов ИСПДн;
- обеспечен учёт и хранение съёмных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- обеспечено резервирование технических средств, дублирование носителей информации;
- обеспечена электромагнитная развязка между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны, и информационными цепями;
- обеспечено использование антивирусных средств защиты от вредоносного ПО и криптографических средств защиты информации;
- обеспечено использование СЗИ, позволяющих вести собственные журналы регистрации событий параллельно со встроенными в ИСПДн;
- обеспечено использование межсетевое экранирование как при использовании программных, так и при использовании аппаратных межсетевых экранов;
- каждый пользователь ИСПДн или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения ими своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- разработка и отладка программ осуществляется за пределами ИСПДн на выделенных АРМ;
- все изменения конфигурации технических и программных средств ИСПДн производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- работниками Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## **9. Контроль эффективности СЗПДн**

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 же прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль эффективности СЗПДн может проводиться как администраторами безопасности 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 Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их компетенции.

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

Оценка эффективности СЗПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

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

Ответственным за разработку мер защиты ПДн и контроль за обеспечением безопасности ПДн является директор Учреждения. Директор может делегировать часть полномочий по обеспечению безопасности ПДн путём издания приказа.

Сфера ответственности директора включает в себя следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- разработка, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности ПДн;
- контроль защищённости ИСПДн КЦСОН от УБПДн;
- обучение и информирование пользователей ИСПДн о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда работникам этих организаций предоставляется доступ к объектам защиты ПДн, с этими организациями заключается соглашение о конфиденциальности либо соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн.

## **11. Модель нарушителя безопасности**

Под нарушителем в Учреждении понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты ПДн.

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

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

Классификация нарушителей представлена в моделях угроз безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения для каждой ИСПДн.

## **12. Модель угроз безопасности**

Для ИСПДн Учреждения выделяются следующие основные категории угроз безопасности ПДн:

1. угрозы от утечки по техническим каналам;
2. угрозы несанкционированного доступа к информации:
  - угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путём физического доступа к элементам ИСПДн;
  - угрозы хищения, несанкционированной модификации или блокирования информации путём НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
  - угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в её 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.

## **13. Механизм реализации Концепции**

Реализация Концепции должна осуществляться на основе перспективных программ и планов Учреждения, которые составляются на основании:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- нормативных и руководящих документов Федеральной службы безопасности Российской Федерации;
- нормативных и руководящих документов Федеральной службы по техническому и экспортному контролю Российской Федерации;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

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

Реализация Концепции безопасности ПДн в ИСПДн Учреждения позволит:

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

Осуществление этих мероприятий обеспечит создание единой и целостной системы информационной безопасности ИСПДн и создаст условия для её дальнейшего совершенствования.



## 15. Ответственность

1. При работе с персональными данными работники Учреждения обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов персональных компьютеров или терминалов.

2. Работники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение, ознакомлены с процедурой наложения дисциплинарных взысканий на работников, которые нарушили настоящую Концепцию и процедуры безопасности персональных данных.

3. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководителю подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

4. Пользователи ИСПДн, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

## Список использованных источников

1. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
4. Указ Президента Российской Федерации от 06 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781;
3. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утверждены постановлением Правительства Российской Федерации от 06 июля 2008 г. № 512;
4. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;
5. Порядок проведения классификации информационных систем персональных данных, утвержденный приказом Федеральной службы по техническому и экспортному контролю Российской Федерации, Федеральной службы безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20;
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора Федеральной службы по техническому и экспортному контролю Российской Федерации 15 февраля 2008 г.;
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора Федеральной службы по техническому и экспортному контролю Российской Федерации 15 февраля 2008 г.;
8. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, утверждены директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23 декабря 2009 г.;
9. Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено приказом Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 г. № 58;
10. Требования о защите информации, содержащейся в информационных системах общего пользования, утверждены приказом Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489.