

Краевое государственное бюджетное учреждение здравоохранения
«Князе-Волконская районная больница» министерства
здравоохранения Хабаровского края



УТВЕРЖДАЮ

Главный врач «Князе-
Волконской РБ»
Т.Г.Ларионова

2013 г.

Концепция информационной безопасности информационных
систем персональных данных КГБУЗ «Князе-Волконская РБ»

ВВЕДЕНИЕ

Настоящая Концепция информационной безопасности ИСПДн КГБУЗ «Князе-Волконская РБ» (Далее - Учреждения) разработана на основе Концепции, разработанной Министерством здравоохранения и социального развития РФ, является документом, в котором определена система взглядов на обеспечение информационной безопасности Учреждения.

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

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения. 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 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.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждений, 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.

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 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 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.

Область применения Концепции распространяется на все учреждения здравоохранения, социальной сферы, труда и занятости, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

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

Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения, в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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 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.

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.

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).

Стадии создания СЗПДн включают:
предпроектная стадия включает предпроектное обследование ИСПДн;
стадия проектирования включает разработку СЗПДн в составе ИСПДн;
стадия ввода в действие СЗПДн включает опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:
План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;
План мероприятий по контролю обеспечения защиты ПДн;
Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;
Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
Должностная инструкция администратора безопасности ИСПДн;
Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
Инструкция на случай возникновения внештатной ситуации;
Рекомендации по использованию программных и аппаратных средств защиты информации.

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

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Учреждения.

2. Задачи СЗПДн

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

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:

а) к информации, циркулирующей в ИСПДн;
б) средствам вычислительной техники ИСПДн;
в) 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.

3. Объекты защиты

3.1. Перечень информационных систем

В Учреждении производится обработка персональных данных в информационных системах обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки.

3.2. 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, подлежащих защите в ИСПД.

Объекты защиты включают:

- 1) Обрабатываемая информация.
- 2) Технологическая информация.
- 3) Программно-технические средства обработки.
- 4) Средства защиты ПДн.

- 5) Каналы информационного обмена и телекоммуникации.
- 6) Объекты и помещения, в которых размещены компоненты ИСПДн.

4.Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник Учреждения, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

1. Администратор ИСПДн. Сотрудники Учреждения, 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.

2. Программист-разработчик ИСПДн. Сотрудники Учреждения или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных 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.

3. Оператор ИСПДн. Сотрудники подразделений Учреждения участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

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

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.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ПДн ИСПДн Учреждения 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.

Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн Учреждения 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.

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

Системность

Системный подход к построению СЗПДн Учреждения предполагает учет 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 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.

Комплексность

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.

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 невязанных областях.

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.

Непрерывность защиты ПДн

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.

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.

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.

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 ее 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 счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

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.

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.

Принцип минимизации 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 объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

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

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.

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.

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 трудозатрат 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.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

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.

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.

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.

6. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться 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).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

Законодательные (правовые) меры защиты

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.

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

Морально-этические меры защиты

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.

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.

Организационные (административные) меры защиты

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.

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.

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

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 Учреждения в целом;

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

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.

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 так же 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.

Организационные меры должны:

предусматривать регламент информационных отношений, исключая 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.

Организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;
- порядок допуска сотрудников 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 пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);
- инструкция пользователя при возникновении внештатных ситуаций.

Физические меры защиты

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.

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, исключая нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

Аппаратно-программные средства защиты ПДн

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.).

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 Учреждения;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности; криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) 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;

в ИСПДн Учреждения разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;

все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (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.).

специалистами Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Контроль эффективности системы защиты ИСПДн Учреждения

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.

Контроль 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 ФСТЭК России и ФСБ России в пределах их компетенции.

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

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

8. Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель Учреждения. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя 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 Компании 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.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн». Подготовка типовых вариантов этих соглашений осуществляется совместно с Юридическим отделом.

9. Модель нарушителя безопасности

Под нарушителем в Учреждении понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

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.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10. Модель угроз безопасности

Для ИСПДн Учреждения выделяются следующие основные категории угроз безопасности персональных данных:

1. Угрозы от утечки по техническим каналам.

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.

11. Механизм реализации Концепции

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.

12. Ожидаемый эффект от реализации Концепции

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.

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