Министерство здравоохранения
Астраханской области
Государственное бюджетное учреждение
здравоохранения Астраханской области
«Областной наркологический диспансер»

УТВЕРЖДАЮ
главный врач ГБУЗ АО «ОНД»

Концепция
информационной безопасности в
автоматизированных информационных
системах ГБУЗ АО «ОНД» от 06.04.2020г.

Оглавление

1. Введение.

1.1. Настоящая Концепция информационной безопасности ИСПДн. ГБУЗ АО «ОНД» (далее – Учреждение), является официальным документом, в котором определена система взаимосвязанных понятий и принципов по обеспечению информационной безопасности реализуемых Учреждением ИПСДн.

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

1.3. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения СЗПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности системы.

1.4. Настоящая Концепция разработана на основе анализа требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопрос защиты ПДн, с учетом современного состояния и стратегии развития информационных технологий, целей, задач и правовых основ создания и эксплуатации информационных систем Учреждения, режимов функционирования, а также на основе анализа угроз ПДн.

1.5. Под информационной защитой ПДн понимается защищенность ПДн 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.

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

1.7. Концепция является методологической основой для:

1.7.1. Формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Учреждения.

1.7.2. 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.

1.7.3. Координации деятельности структурных подразделений Учреждения при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн.

1.7.4. Разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Учреждения.

1.8. Область применения Концепции распространяется на подразделения Учреждения, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

1.9. Правовой основой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Термины и определения.

В настоящем документе используются следующие термины:

ИСПДн- информационная система персональных данных.

СЗПДн - система защиты персональных данных.

ПДн — персональные данные.

НСД — несанкционированный доступ.

ТС - технические средства.

ПО — программное обеспечение.

ОИТ — отдел информационных технологий.

СЗИ — средства защиты информации.

МРМ — мобильное рабочее место.

АРМ — автоматизированное рабочее место.

ЭП — электронная подпись.

СКЗИ — средство криптографической защиты.

3. Общие положения.

3.1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения СЗПДн Учреждения, в соответствии с перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

3.2. 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 других неправомерных действий с ними.

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

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

- организационные меры;
- 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);
- используемые в информационной системе информационные технологии.

3.5. Эти меры призваны обеспечить:

3.5.1. Конфиденциальность информации (защита от несанкционированного ознакомления);

3.5.2. Целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

3.5.3. Доступность информации (возможность за доступное время оказать требуемую услугу).

3.6. Стадии создания СЗПДн включают:

3.6.1. Предпроектное обследование ИСПДн;

3.6.2. Стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

3.6.3. Стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

3.7. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности следующих организационно-распорядительных документов:

3.7.1. План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

3.7.2. Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

3.7.3. Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

3.7.4. Должностная инструкция администратора безопасности ИСПДн;

3.7.5. Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

3.7.6. Инструкция на случай возникновения внештатной ситуации.

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

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

4. Концепция информационной безопасности.

4.1. Разработка Концепции информационной безопасности Учреждения осуществляется специалистом по защите информации.

Процедура разработки:

- специалист по защите информации подготавливает проект Концепции путем выработки четкой позиции в решении вопросов информационной безопасности на основе действующего законодательства и потребностей Учреждения в области защиты информации;

- при подготовке проекта специалист по защите информации взаимодействует с сотрудниками отдела информационных технологий Учреждения (далее ОИТ);

- проект документа согласуется с юрисконсультом, заместителем главного врача по общим вопросам и заместителем главного врача по ОМКР;

Для разработки Концепции могут быть привлечены сторонние организации или специалисты, имеющие соответствующие квалификации и разрешения на деятельность в этой области.

4.2. Реализация Концепции информационной безопасности должна обеспечиваться четким управлением и реальной поддержкой со стороны руководства инициатив в области безопасности, ответственным исполнением каждым сотрудником правил в области защиты информации, утвержденных в Учреждении, а также соблюдением этики, моральных норм и правил.

4.3. 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 информации.

4.4. Отдел информационных технологий осуществляет программно-техническое и консультационное сопровождение реализации Концепции согласно Положению об ОИТ.

4.5. Документальное оформление.

Концепция информационной безопасности утверждается приказом главного врача Учреждения, издается и надлежащим образом доводится до сведения всех сотрудников Учреждения.

4.6. Пересмотр и оценка.

Пересмотр Концепции осуществляется комиссией по защите персональных данных при изменении законодательства, выявлении существенных инцидентов нарушения информационной безопасности, не предусмотренных Концепцией, появлении новых уязвимостей, по представлению специалиста по защите информации, сотрудников ОИТ Учреждения, юрисконсульта, а также изменений организационной или технологической инфраструктуры, но не реже одного раза в три года.

При внесении изменений в положения Концепции учитываются:

- уровень развития и внедрения информационных технологий в телекоммуникационной отрасли;

- рекомендации российских и международных профильных организаций по информационной безопасности и защите ПДн;

- рекомендации Консультационного совета при уполномоченном органе по защите прав субъектов ПДн.

Для пересмотра и оценки Концепции могут привлекаться внешние консультанты и организации, специализирующиеся и имеющие компетенции в области безопасности, а также соответствующие органы.

5. Цели и 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:

5.2.1. Защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования информационной системой и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

5.2.2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций, 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 информации, используемым в ИСПДн;

5.2.3. Возможность ведения В ИСПДн журналов или протоколов критически важных событий, созданных пользователями и влияющих на сохранность ПДн.;

5.2.4. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановления в случае нарушения;

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

5.2.6. Защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

5.2.7. Защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

5.2.8. Обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

5.2.9. 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;

5.2.10. Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидации последствий нарушения безопасности ПДн.

6. Взаимодействие со сторонними лицами и организациями.

Взаимодействие со сторонними лицами и организациями по вопросам реализации информационной безопасности, доступа к информационным системам Учреждения, а также привлечение сторонних организаций к обработке информации (аутсорсинг) определяются *Положением о взаимодействии со сторонними лицами и организациями*.

7. Перечень информационных систем.

В Учреждении производится обработка персональных данных в информационных системах обработки персональных данных. Перечень ИСПДн определяется на основании Акта по результатам внутренней проверки.

8. Объекты защиты.

8.1. Объектами защиты являются: информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащих защите, определен в Перечне персональных данных, подлежащих защите в ИСПДн.

8.2. Объекты защиты включают:

8.2.1. Обрабатываемую информацию.

8.2.2. Технологическую информацию.

5.2.3 Программно-технические средства обработки.

8.2.4. Средства защиты ПДн.

8.2.5. Каналы информационного обмена и телекоммуникации.

8.2.6. Объекты и помещения, в которых размещены компоненты ИСПДн.

9. Классификация пользователей ИСПДн.

9.1. 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.

9.2. Пользователи ИСПДн делятся на три основные категории:

9.2.1. 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.

9.2.2. Программист — разработчик ИСПДн. Сотрудники предприятия 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.

9.3. Оператор ИСПДн — сотрудники подразделений Учреждения, участвующие в процессе эксплуатации ИПСДн. Оператор ИПСДн — сотрудник, обладающий следующим уровнем доступа:

- обладает всеми необходимыми артибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

9.4. 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.

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

10. Основные принципы построения системы комплексной защиты информации.

Построение системы обеспечения безопасности ПДн ИСПДн Учреждения и ее функционирование должны осуществляться в соответствии с 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 невзаимосвязанных 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 — это 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.

11. Типы угроз и уровни защищенности.

Типы угроз и уровни защищенности ПДн в ИСПДн определяются согласно Постановлению Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановлением устанавливаются четыре уровня защищённости персональных данных при их обработке в информационных системах и требования для каждого из них.

Документ позволяет определить требуемый уровень защищённости персональных данных, что в значительно упрощает процедуру определения необходимых и достаточных мер по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

12. Общие методы обеспечения безопасности персональных данных.

12.1. Классификация методов обеспечения безопасности персональных данных.

Методы обеспечения безопасности ПДн разделяются на:

- административно-правовые;

- организационно-технические;

- экономические.

По времени применения методы обеспечения безопасности ПДн разделяются на:

- превентивные;

- восстановительные.

Административно-правовые методы.

К административно-правовым методам защиты относятся нормы действующего законодательства Российской Федерации в области персональных данных и внутренние организационно-распорядительные документы Учреждения, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерной обработке ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

Основными направлениями этой деятельности Учреждения являются:

- разработка, внесение изменений и дополнений в политику информационной безопасности в части защиты ПДн и поддерживающие её документы;

-регламентация процессов обработки ПДн;

-определение ответственности за нарушения в области обеспечения безопасности ПДн;

назначение и подготовка должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн;

-закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения безопасности ПДн;

- разработка и принятие документов, устанавливающих ответственность структурных подразделений и сотрудников, а также взаимодействующих

юридических лиц, за несанкционированный доступ к ПДн, противоправное их раскрытие или использование в преступных и корыстных целях;

- контроль знания и соблюдения пользователями ИСПДн, требований организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;

-проведение постоянного анализа эффективности и достаточности принимаемых мер и применяемых средств защиты ПДн, разработка и реализация предложений по совершенствованию СЗПДн.

Организационно- технические методы.

Организационно- технические методы защиты основаны на использовании организационных мер, различных программных, аппаратных и программно-аппаратных средств, входящих в состав СЗПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

- строгий учет всех подлежащих защите ресурсов (персональных данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т. д.);

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

- своевременного обнаружения фактов НСД к ПДн;

- недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

- постоянного контроля за обеспечением уровня защищенности ПДн.

Экономические методы.

Экономические методы обеспечения безопасности ПДн включают в себя:

- разработку Учреждением программ обеспечения безопасности ПДн и определение порядка их финансирования.

- разработку Учреждением мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки ПДн.

Превентивные методы.

Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации

ИПСДн комплекса организационных, технических и технологический мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИПСДн.

Восстановительные методы.

Планирование восстановительных методов определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

12.2. Основные этапы работ по обеспечению безопасности персональных данных входят, в частности, следующие:

- определение объектов защиты;
- установление целей защиты объектов;
- установление требований к системе защиты персональных данных;
- определения порядка контроля и надзора.

Основным объектом защиты являются персональные данные.

Персональные данные могут иметь различные формы представления (бумажная, электронная, записи и поля записей баз данных, электромагнитные волны и поля, излучения и т. д.), каждая из которых является объектом защиты.

Формы представления персональных данных связаны с различными ресурсами информационной системы персональных данных, которые, в свою очередь, могут порождать объекты защиты.

Используемые в информационной системе персональных данных средства защиты информации являются объектами защиты.

Информация о методах и средствах обеспечения безопасности персональных данных содержит сведения, которые являются объектами защиты, в частности, к каким объектам могут быть отнесены парольная и аутентифицирующая информация, ключевая информация.

Установление целей защиты объектов связано с установлением характеристик безопасности для каждого из определенных объектов защиты.

Определение угроз объектам защиты информации проводится путем формирования модели угроз и модели нарушителя. При этом модель нарушителя

формируется как составная часть модели угроз, определяющая возможные специфические угрозы — атаки.

Установление требований к системе защиты персональных данных основано на формировании моделей угроз нарушителя.

В первую очередь устанавливаются общие требования к организационным мерам.

Далее на основе моделей угроз и нарушителя, сформированных в соответствии с нормативными и методическими рекомендациями ФСТЭК России, определяются требования к средствам защиты информации, входящими в зону ответственности ФСТЭК России, а также требования к поддерживающим эти средства организационным мерам.

Процесс формирования требований к системе защиты персональных данных заканчивается, если выполнение установленных требований нейтрализует все угрозы, перечисленные в моделях угроз нарушителя.

Если выполнение установленных требований нейтрализует не все угрозы, перечисленные в моделях угроз и нарушителя, сформированных в соответствии с требованиями нормативными и методическими рекомендациями ФСТЭК России, на основе моделей и угроз нарушителя, сформированных в соответствии с нормативными документами ФСБ России, определяются требования к средствам защиты информации, входящими в зону ответственности ФСБ России, а также требования к поддерживающим эти средства организационным мерам.

Контроль и надзор за обеспечением защиты персональных данных осуществляются на периодической основе с использованием имеющихся средств и формированием соответствующих документов и актов. Контроль и надзор должны осуществляться на основе принципа достаточности и минимально необходимого вмешательства с целью недопущения прерываний процессов создания, хранения и обработки информации, содержащей ПДн.

13. Модель нарушителя безопасности.

Основным источником угроз персональных данных является нарушитель.

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

- внешние нарушители —организации или физические лица, не имеющие право пребывать 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.

Основными мотивами нарушения безопасности персональных данных могут быть:

- месть;

- достижение денежной выгоды, в том числе за счет продажи полученной информации;

- хулиганство и любопытство;

- профессиональное самоутверждение.

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

14. Модель угроз безопасности.

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

1) угрозы по техническим каналам;

2) угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИПСДн;

- 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 непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также угроз неантропогенного (ударов молний, пожаров, наводнений и т. п.) характера;

- угрозы преднамеренных действий и 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.

15. Основные мероприятия по обеспечению безопасности персональных данных.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн Учреждением назначается структурное подразделение (ОИТ) и должностное лицо (специалист по защите информации), ответственное за обеспечение безопасности ПДн.

Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

- мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;

- мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;

- мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн. Структура, состав и основные функции СЗПДн определяются с учетом типа угроз и уровня защищенности.

Перечень реализуемых мероприятий по защите ПДн при их обработке в специальных ИСПДн Учреждения определяется на основании анализа актуальности угроз, рисков безопасности ПДн и профилей защиты ПДн для ИСПДн Учреждения, в соответствии с нормативными и методическими документами ФСБ России и ФСТЭК России.

ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, поэтому целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и

Федеральной службой безопасности Российской Федерации в пределах их полномочий.

В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю:

- осуществляется обеспечение защиты (некриптографическими методами) информации;

- проводятся мероприятия по предотвращению утечки информации по техническим каналам;

- проводятся мероприятия по предотвращению несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней.

В соответствии с нормативными документами Федеральной службы безопасности Российский Федерации:

- устанавливаются особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах;

- проводятся мероприятия по обнаружению компьютерных атак.

Мероприятия по обеспечению безопасности ПДн включают в себя:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и

(или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных, идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

16. Принцип оценки контроля эффективности системы защиты персональных данных Учреждения.

В соответствии с принципом обязательности контроля (раздел 10) выполняются следующие виды контроля эффективности системы защиты персональных данных:

- внутренний контроль;

- государственный контроль.

Внутренний контроль эффективности системы защиты ПДн осуществляется Учреждением с целью поддержания заданного уровня эффективности СЗПДн, в соответствии с документированными методиками. Внутренний контроль включает:

- мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

- контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-распорядительных документов Учреждения, сформулированных на основе анализа рисков нарушения безопасности ПДн, договорных требований).

Оценка эффективности СЗПДн реализуется в виде аттестации или декларирования соответствия требованиям безопасности по ПДн.

Декларирование вводится по факту ввода в эксплуатацию ИПСДн.

Ввод в эксплуатацию ИСПДн производится в соответствии с документально оформленными требованиями по безопасности ПДн (техническими условиями), разрабатываемыми Учреждением в соответствии с требованиям законодательства и нормативно-методических документов федеральных органов исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

Факт ввода в эксплуатацию ИСПДн в соответствии с техническими условиями оформляется Актом ввода в эксплуатацию и утверждается приказом по Учреждению.

Государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российский Федерации в области персональных данных осуществляется Роскомнадзором.

Контроль и надзор за выполнением требований безопасности персональных данных при их обработке в ИСПДн осуществляются ФСБ России и ФСТЭК России в пределах их полномочий.

17. Ожидаемый эффект от реализации Концепции.

17.1. Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценивать состояние безопасности ИСПДн, выявлять источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разрабатывать распорядительные и нормативно — методические документы применительно к ИСПДн;

- проводить классификацию, аттестацию ИСПДн;

- проводить организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

- обеспечивать необходимый уровень безопасности объектов защиты.

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

18. Нормативно — методическое обеспечение.

18.1. Федеральные законы РФ.

Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Федеральный закон от 01 июля 2011 г. № 261-ФЗ «О внесении изменений в ФЗ «О персональных данных».

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981г. с изменениями и дополнениями).

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001г №195-ФЗ.

Трудовой кодекс РФ - Глава 14. Защита персональных данных работника от 30.12.2001г №197-ФЗ.

18.2. Указы президента РФ.

Доктрина информационной безопасности РФ 9 сентября 2000 г. №Пр-1895.

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при

использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

18.3. Постановления Правительства РФ.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

18.4. Нормативные документы ФСТЭК России.

Положение по аттестации объектов информатизации по требованиям безопасности информации.

Приказ Федеральной службы по техническому и экспортному контролю
от 18 февраля 2013 г. N 21
"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

18.5. Нормативные документы Роскомнадзора.

Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.