Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение   
высшего образования «Национальный исследовательский университет   
«Московский институт электронной техники»

Кафедра «Информационная безопасность»

# ПРАКТИЧЕСКОЕ ЗАДАНИЕ №1

по дисциплине«Информационная безопасность /

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выполнили студенты П-32:

Селезнева Валерия  
Утева Александра

Москва, 2021

1. Общие положения

Настоящая «Концепция ИБ» определяет систему взглядов на проблему обеспечения ИБ и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения ИБ.

Законодательной основой настоящей Концепции являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные правовые и правовые акты законодательства Российской Федерации, документы Государственной технической комиссии при Президенте Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), Федеральной службы по техническому и экспортному контролю (ФСТЭК), а также нормативно-методические материалы и организационно-распорядительные документы, отражающие вопросы обеспечения ИБ.

Концепция учитывает современное состояние и ближайшие перспективы развития ИС «Pharmacy», цели, задачи и правовые основы ее создания и эксплуатации, режимы функционирования данной системы, а также общий анализ угроз безопасности для ИР.

Основные положения и требования Концепции распространяются на все структурные подразделения, в которых осуществляется автоматизированная обработка информации, содержащей сведения, составляющие банковскую, коммерческую, служебную тайну, или персональные данные, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения ИБ и подведомственных территориальных организациях;

- принятия управленческих решений и разработки практических мер по воплощению политики ИБ и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ИБ;

- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации ИC с соблюдением требований обеспечения ИБ;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения ИБ.

Требования настоящей Концепции распространяются только на обеспечение ИБ, не составляющей государственную тайну. Концепция не регламентирует вопросы охраны помещений и обеспечения сохранности и физической целостности компонентов ИС, защиты от стихийных бедствий, сбоев в системе энергоснабжения, а также меры по обеспечению личной безопасности персонала и клиентов ООО «Pharmacy».

Научно-методической основой Концепции является системный подход, предполагающий проведение исследований, разработку системы ЗИ и процессов ее обработки в ИС с единых методологических позиций с учетом всех факторов, оказывающих влияние на ЗИ, и с позиции комплексного применения различных мер и средств защиты.

При разработке Концепции учитывались основные принципы создания комплексных систем ИБ, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам ИБ, а также текущее состояние и перспективы развития ИТ.

Основные положения Концепции базируются на качественном осмыслении вопросов ИБ и не концентрируют внимание на экономическом анализе рисков и обосновании необходимых затрат на ЗИ.

Информационная безопасность достигается в результате обеспечения целостности, доступности и конфиденциальности в рамках ИС.

Целостность достигается путем разработки и внедрения технологий контроля и восстановления целостности ИР, средствами разграничения полномочий, средствами защиты от НСД к ИР и каналам связи, физической охраной технических средств ИС и носителей информации и другими организационно-техническими мерами, регламентирующими доступ к ИР ИС.

Доступность достигается путем защиты от НСД к ИС, резервирования программно-технических средств, защиты от перегрузки оборудования, дублирования каналов передачи данных в сети, а также организационно-технологическими мерами.

Конфиденциальность достигается путем применения сертифицированных средств ЗИ от НСД (в том числе криптографических), реализацией правил разграничения доступа к ИР, а также организационными мерами и мерами дисциплинарного, административного и иного воздействия в соответствии с законодательством Российской Федерации по предотвращению разглашения информации конфиденциального характера и неправомерных действий со стороны лиц, имеющих право доступа к информации конфиденциального характера.

**Ответственность**

Ответственность за реализацию и соблюдение требований, изложенных в настоящей Концепции, возлагается:

- на все категории пользователей ИС «Pharmacy»

Контроль над реализацией, а также координацию работ по подготовке Концепции ИБ, пересмотр и дополнение положений возлагается на подразделение, отвечающее за обеспечение ИБ в соответствии с его функциональными обязанностями и полномочиями, определенными нормативными актами ООО «Pharmacy».

Корректировка Концепции производится по мере необходимости в соответствии с установленным порядком.

**2. Объекты защиты:**

Основными объектами информационной безопасности являются:

• информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, представленные в виде документов и массивов информации, независимо от формы и вида их представления;

• процессы обработки информации в АС - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков и пользователей системы и ее обслуживающий персонал;

• информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты АС.

**2.1 Назначение, цели создания и эксплуатации ИС как объекта информатизации**

ИС предназначена для автоматизации деятельности должностных лиц

ООО «Pharmacy». Создание и применение ИС преследует следующие цели:

- повышение качества работы сотрудников АО «Pharmacy»

- автоматизация процесса регистрации поступающих лекарств в аптеку

- электронное хранение информации о лекарствах и постоянных посетителях

**2.2 Структура, состав и размещение основных элементов АС, информационные связи с другими объектами АС**

Представляет собой главный ПК, где храниться вся конфиденциальная информация, и двух ПК, которые подключены к главному.

В АС циркулирует информация разных категорий. Защищаемая информация может быть совместно использована различными пользователями с равными правами доступа из одинаковых подсетей единой вычислительной сети.

Комплекс технических средств АС включает средства обработки данных (ПЭВМ для взаимодействия с АС и хранения конфиденциальной информации), без возможности выхода в глобальные сети (кабельная система, мосты, шлюзы, модемы и т.д.).

**3. Цели и задачи обеспечения ИБ:**

- цели защиты;

- основные задачи системы обеспечения безопасности информации;

**3.1. Интересы затрагиваемых при использовании ИС субъектов информационных отношений**

Субъектами правоотношений при использовании ИС и обеспечении ИБ являются:

- Компания как собственник ИС;

- подразделения, обеспечивающие эксплуатацию системы автоматизированной обработки информации;

- должностные лица и сотрудники ООО «Pharmacy», как пользователи и поставщики информации в ИС в соответствии с возложенными на них функциями;

- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в ИС;

- другие юридические и физические лица, задействованные в процессе создания и функционирования ИС;

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) определенной части информации;

- достоверности (полноты, точности, адекватности, целостности) информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

- своевременного доступа (за приемлемое для них время) к необходимой им информации;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

**3.2 Цель и задачи концепции информационной безопасности**

**Главная** **цель** обеспечения безопасности информации является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы.

**Основными задачами** обеспечения безопасности информации являются:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба и нарушению нормального функционирования и развития ИС;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности подразделений по обеспечению защиты информации;

- создание и применение защищенных информационных объектов и АИС, центров обработки защищаемой информации;

создание механизмов управления системой информационной безопасности.

**Основной целью системы защиты ПДн** является минимизация ущерба от возможной реализации угроз безопасности ПДн.

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

- защиту от вмешательства в процесс функционирования 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, то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИС;

б) к средствам вычислительной техники;

- регистрацию действий пользователей при использовании защищаемых ресурсов 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 программных средств, а также защиту системы от внедрения несанкционированных программ;

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

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

**3.3 Основные пути достижения целей защиты**

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов системы;

- регламентацией процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников АО «Библиотека», использующих АС;

- назначением и подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам АС;

- четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- персональной ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;

- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС.

**4. Основные угрозы ИБ:**

- угрозы информационной безопасности и их источники;

- пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности;

- умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала;

- утечка информации по техническим каналам;

- неформальная модель возможных нарушителе

**Угрозы информационной безопасности и их источники**

Наиболее опасными угрозами ИБ являются:

- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную информацию ограниченного распространения, а также персональных данных;

- нарушение работоспособности (дезорганизация работы) ИС, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов ИС, а также фальсификация (подделка) документов.

**4.1 Угрозы нарушения конфиденциальности информации**

**и все угрозы которые из модели угроз-сами названия угроз**

**-** Нарушение конфиденциальности информации путем передачи конфиденциальной информации третьим лица.

**-** Нарушение конфиденциальности информации путем передачи информации о юридическом лице третьим лица.

**4.2 Угрозы нарушения целостности информации**

- Неправомерное использование декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера

- Нарушение целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр

- Нарушение целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём.

**4.3 Источники угроз безопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **вида** | **Виды**  **нарушителя** | **Категории**  **нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Поставщики вычислительных услуг, услуг связи | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия. |
| 2 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием;  Непреднамеренные, неосторожные или неквалифицированные действия |
| 3 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Передача конфиденциальной информации третьим лицам;  Передача информации о юридическом лице третьим лицам;  Получение финансовой или иной материальной выгоды;  Любопытство или желание самореализации (подтверждение статуса);  Непреднамеренные, неосторожные или неквалифицированные действия;  Месть за ранее совершенные действия |
| 4 | Авторизованные пользователи систем и сетей | Внутренний | Передача конфиденциальной информации третьим лицам;  Передача информации о юридическом лице третьим лицам;  Получение финансовой или иной материальной выгоды;  Любопытство или желание самореализации (подтверждение статуса);  Непреднамеренные, неосторожные или неквалифицированные действия;  Месть за ранее совершенные действия |
| 5 | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки |
| 6 | Отдельные физические лица (хакеры) | Внутренний | Передача конфиденциальной информации третьим лицам;  Передача информации о юридическом лице третьим лицам;  Получение финансовой или иной материальной выгоды;  Любопытство или желание самореализации (подтверждение статуса); |

**4.4Пути реализации угроз ИБ**

1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций

1.2. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.

1.3. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.

2.1. Эксплуатация уязвимостей компонентов систем и сетей при локальной атаке.

2.2. Несанкционированное подключение внешних устройств.

2.2. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)

3. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.

4.1. Несанкционированное создание учетных записей или кража существующих учетных данных

4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети

5.1. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи

5.2 Эксплуатация уязвимостей ПО к повышению привилегий.

6.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.

6.2. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей

6.3. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков

7. Вывод информации через съемные носители

8.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках

8.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа

8.3. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей

**4.6 По техническим каналам**

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств ИС и линий передачи информации;

- наводки информативного сигнала, обрабатываемого ИС, на провода и линии, выходящие за пределы контролируемой зоны, в т.ч. на цепи заземления и электропитания;

- изменения тока потребления, обусловленные обрабатываемыми ИС информативными сигналами;

- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав ИС, или при наличии паразитной генерации в узлах (элементах) ИС;

- радиоизлучения или электрические сигналы от внедренных в ИС и выделенные помещения специальных электронных устройств перехвата информации ("закладок"), модулированные информативным сигналом;

- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

и т.д.

В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

- космические средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций и приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации;

- стационарные средства, размещаемые в зданиях;

- автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

**5. Основные положения технической политики в области обеспечения ИБ:**

5.1 Техническая политика в области ИБ

Реализация технической политики в области обеспечения ИБ должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической политики обеспечения ИБ ИС являются:

- обеспечение ЗИ ИР от хищения, утраты, утечки, уничтожения, искажения или подделки за счет НД и специальных воздействий;

- обеспечение ЗИ от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

В рамках указанных направлений технической политики обеспечения ИБ осуществляются:

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;

- реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

- учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль за НСД и действиями персонала;

- предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок;

- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

- надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение; - снижение уровня и информативности побочных электромагнитных излучений и наводок, создаваемых различными элементами автоматизированных подсистем;

- электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы контролируемой зоны;

- активное зашумление в различных диапазонах;

- противодействие оптическим и лазерным средствам наблюдения и т.д.

**6. Основные принципы построения системы комплексной защиты информации:**

**Принцип обязательности ограничений:**

* + Противодействие угрозам безопасности информации всегда налагает ограничения организационного и технического характера по отношению к пользователям и обслуживающему персоналу корпоративной сети.

**Принцип прозрачности:**

* + Основное назначение КС организации - обеспечение производственных потребностей пользователей организации, при этом сервисами КС и системой ИБ организации пользуются специалисты различной квалификации;

**Принцип превентивности:**

* + Устранение последствий проявления угроз требует больших финансовых, временных и материальных затрат, чем своевременное устранение уязвимостей КС и предотвращение угроз.

**Принцип оптимальности:**

* + Оптимальный выбор соотношения между различными методами и способами защиты позволит в значительной степени сократить расходы на создание системы ИБ.

**Принцип адекватности:**

* + Дифференциация решений в зависимости от важности, частоты и вероятности возникновения угроз безопасности, степени конфиденциальности информации и ее коммерческой стоимости.

**Принцип адаптивности:**

* + СОИБ должна строиться с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности информации и т.д.

**7. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов:**

**Средства защиты информации от НСД**

**Подсистема идентификации, проверки подлинности и контроля доступа субъектов в систему СЗПДн "** **Pharmacy "**   
- идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно  
-постоянного действия длиной не менее шести буквенно-цифровых символов

**Подсистема регистрации и учета входа (выхода) субъектов доступа в (из) систему (узел сети) СЗПДн "** **Pharmacy "**   
- указывание даты и времени входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная (при НСД);

**Подсистема целостности программных средств и обрабатываемой информации СЗПДн "** **Pharmacy "**   
- проверка целостности СЗИ НСД при загрузке системы по наличию имен (идентификаторов) компонент СЗИ

- обеспечение отсутствия в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации

**Подсистема наличия средств восстановления СЗИ НСД СЗПДн " Pharmacy "**   
- наличие средств восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности

**Средства антивирусной защиты информации**

* Генерация данных аудита
* Ассоциация идентификатора пользователя
* Просмотр аудита
* Ограниченный просмотр аудита
* Выборочный просмотр аудита
* Управление режимом выполнения функций безопасности
* Управление данными ФБО
* Роли безопасности
* Базовое обнаружение КВ
* Проверка файлов, полученных по каналам передачи данных
* Методы анализа
* Выполнение проверок
* Запуск выполнения проверок внешней программой
* Удаление КВ

**Средства межсетевой защиты**

* Сигналы нарушения безопасности
* Генерация данных аудита
* Просмотр аудита
* Избирательный аудит
* Аутентификация до любых действий пользователя
* Идентификация до любых действий пользователя
* Полное управление информационными потоками
* Простые атрибуты безопасности
* Управление режимом выполнения функций безопасности
* Управление данными функций безопасности
* Спецификация функций управления
* Роли безопасности
* Управление атрибутами безопасности
* Ручное восстановление

**8. Перечень мероприятий по обеспечению ИБ.**

Для реализации основных положений настоящей Концепции целесообразно провести (осуществить) следующие мероприятия:

- создать в центральном аппарате, во всех территориальных управлениях и подведомственных организациях компании подразделения технической ЗИ в ИС и/или ввести ответственных (из числа сотрудников) за ИБ в структурных подразделениях, территориальных управлениях и подведомственных организациях компании, определить их задачи и функции на различных стадиях создания, развития и эксплуатации ИС и системы ЗИ;

- для снижения затрат на создание системы защиты и упрощения категорирования и аттестации подсистем ИС рассмотреть возможность внесения изменений в конфигурацию сетей и СВТ, технологии обработки, передачи и хранения (архивирования) информации;

- определить порядок приобретения и использования сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации; образцов технических средств, прошедших специальные исследования, в соответствии с требованиями предписания на эксплуатацию, а также сертифицированных средств ЗИ;

- уточнить конкретные требования к ИС, включаемые в ТЗ на разработку проектов ИС;

- определить возможность использования в ИС имеющихся сертифицированных средств ЗИ;

- произвести закупку сертифицированных образцов и серийно выпускаемых технических и программных средств ЗИ и их внедрение на рабочих станциях и файловых серверах ИС с целью контроля за изменением конфигурации аппаратных и программных средств и действиями пользователей;

- определить степень участия персонала в обработке (передаче, хранении, обсуждении) информации, характер его взаимодействия между собой и с подразделениями (или ответственными сотрудниками по ИБ) по ЗИ;

- произвести разработку и реализацию разрешительной системы доступа пользователей и эксплуатационного персонала ИС или иного объекта информатизации к обрабатываемой информации;

- произвести разработку организационно-распорядительной и рабочей документации по эксплуатации объекта информатизации в защищенном исполнении, а также средств и мер ЗИ в ИС, регламентирующих процессы допуска пользователей к работе с ИС, разработки, приобретения и использования программного обеспечения на рабочих станциях и серверах, порядок внесения изменений в конфигурацию аппаратных и программных средств при ремонте, развитии и обслуживании СВТ, порядок применения и администрирования средств ЗИ, на основе Регламентов по ИБ;

- для снижения риска перехвата в сети с других рабочих станций имен и паролей привилегированных пользователей (в особенности администраторов средств защиты и БД) организовать их работу в отдельных сегментах сети (VLan), шире применять сетевые устройства типа switch, не использовать удаленных режимов конфигурирования сетевых устройств (маршрутизаторов, концентраторов и т.п.);

**Приложение 1**. Перечень нормативных документов, регламентирующих деятельность в области ЗИ.

1. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) информационное сообщение об утверждении требований к средствам антивирусной защиты от 30 июля 2012 г. N 240/24/3095
3. Федеральная служба по техническому и экспортному контролю. Информационное сообщение. Об утверждении требований к межсетевым экранам. От 28 апреля 2016 г. N 240/24/1986
4. Федеральная служба по техническому и экспортному контролю Информационное сообщение. Об утверждении требований к межсетевым экранам. От 28 апреля 2016 г. N 240/24/1986
5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Информационное письмо. Об утверждении требований к системам обнаружения вторжений
6. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Утверждён ФСТЭК России 12 сентября 2016 г. Методический документ профиль защиты межсетевых экранов типа «Б» пятого класса защиты ИТ.МЭ.Б5.ПЗ
7. Утвержден ФСТЭК России 14 июня 2012 г. Методический документ профиль защиты средств антивирусной защиты типа «Б» пятого класса защиты ИТ.САВЗ.Б5.ПЗ

**Приложение 2**. Список использованных сокращений.

СВТ – средства вычислительной техники

ЗИ – защита информации

ИБ – информационная безопасность

БД – база данных

ИС – информационная система

ИР – информационные ресурсы

АО – акционерное общество

НСД – несанкционированный доступ

ПЭВМ – персональная электронно-вычислительная машина

ПДн – персональные данные

АРМ – автоматизированное рабочее место