МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__8__» ___08_____ 2023 г.

Нормативно-правовое регулирование в сфере информационной безопасности

Методические указания по выполнению практических работ по дисциплине «Нормативно-правовое регулирование в сфере информационной безопасности» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Нормативно-правовое регулирование в сфере информационной безопасности: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 31 с.: Библиогр.: с. 30.

Содержат сведения по вопросам изучения аспектов нормативно-правового регулирования в сфере информационной безопасности для успешной профессиональной деятельности, а также развития в процессе обучения системного мышления, необходимого для решения задач управления в области информационной безопасности.

Методические указания по выполнению практических работ по дисциплине «Нормативно-правовое регулирование в сфере информационной безопасности» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60х84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

Работа №1.

Тема: Организационно-правовые механизмы обеспечения информационной безопасности.

Цель и содержание

Цель организационно-правовых механизмов обеспечения информационной безопасности состоит в создании и поддержании эффективной системы, которая защищает информацию от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Эта система включает в себя применение юридических и организационных инструментов, а также разработку и внедрение политик, процедур, стандартов и контрольных механизмов.

Организационные механизмы обеспечения информационной безопасности включают в себя следующие цели:

1. Разработка политики информационной безопасности: Основная задача состоит в разработке документа, который определяет общие принципы и цели безопасности информации в организации. Политика должна быть четкой, понятной и доступной для всех работников.
2. Установление организационной структуры: Необходимо определить роли и ответственность за обеспечение безопасности информации в организации. Создание команды, отвечающей за информационную безопасность, помогает гарантировать координацию и выполнение мер безопасности.
3. Обеспечение обучения и осведомленности: Организации должны предоставлять обучение и информацию о политике безопасности информации своим сотрудникам. Это позволяет повысить осведомленность о рисках информационной безопасности и способствует принятию правильных решений в процессе работы.
4. Управление доступом: Создание системы управления доступом к информации, которая ограничивает доступ только уполномоченным лицам, является важной составляющей безопасности информации. Включает в себя использование паролей, шифрования данных, аутентификации пользователя и других технических мер безопасности.
5. Регулярное обновление и аудит безопасности: Необходимо периодически обновлять политику безопасности информации, процедуры и технические меры в соответствии с изменяющимися угрозами и требованиями. Проведение аудита безопасности помогает выявить слабые места и предпринять меры по их устранению.

Правовые механизмы обеспечения информационной безопасности включают следующие цели:

1. Законодательное регулирование: Государство разрабатывает и вводит законы и нормативные акты, которые определяют правовой статус информации, устанавливают ответственность за ее нарушение и обеспечивают права и свободы граждан в отношении использования информации.

2. Защита интеллектуальной собственности: Правовые механизмы включают в себя защиту авторских прав, патентов, товарных знаков и других форм интеллектуальной собственности, чтобы предотвратить несанкционированное использование и распространение информации.

3. Конфиденциальность и защита персональных данных: Законы о защите персональных данных регулируют сбор, хранение, использование и передачу личной информации о физических лицах. Это гарантирует конфиденциальность и предотвращает злоупотребление этой информацией.

4. Уголовная ответственность: Законодательство предусматривает уголовную ответственность за преступления, связанные с безопасностью информации, такие как несанкционированный доступ к компьютерным системам, киберпреступления и другие формы нарушения информационной безопасности.

Задание: Улучшение политики информационной безопасности

Описание задания:

Вашей задачей является проведение анализа и разработка улучшенной политики информационной безопасности для организации. При выполнении задания следуйте нижеприведенным шагам:

Шаг 1: Изучение текущей политики информационной безопасности

Ознакомьтесь с существующей политикой информационной безопасности организации. Изучите ее содержание, цели, процедуры и контрольные механизмы.

Шаг 2: Анализ уязвимостей и требований безопасности

Выполните анализ уязвимостей в текущей политике информационной безопасности и сравните ее с современными требованиями безопасности и лучшими практиками. Определите пробелы и слабые места, которые требуют улучшения.

Шаг 3: Разработка обновленной политики информационной безопасности

На основе результатов анализа разработайте обновленную политику информационной безопасности. Включите в нее следующие аспекты:

- Цели и принципы безопасности информации.
- Определение ролей и ответственности в области информационной безопасности.
- Меры по управлению доступом и аутентификации пользователей.
- Процедуры обнаружения и реагирования на инциденты безопасности.

- Требования к обеспечению конфиденциальности и защите персональных данных.

Шаг 4: Внедрение и коммуникация политики

Разработайте план внедрения обновленной политики информационной безопасности. Определите этапы внедрения, ответственных лиц и сроки выполнения. Подготовьте коммуникационные материалы для обучения сотрудников по новой политике.

Шаг 5: Оценка эффективности и аудит политики

Проведите оценку эффективности обновленной политики информационной безопасности. Оцените соответствие политики требованиям безопасности, эффективность контрольных механизмов и принятие политикой сотрудниками организации. Если необходимо, внесите корректировки и повторно проведите аудит.

Результат задания:

В результате задания вы должны представить улучшенную политику информационной безопасности, план ее внедрения в организацию и оценку ее эффективности.

Контрольные вопросы:

1. Что такое организационно-правовые механизмы обеспечения информационной безопасности?
2. Какие основные цели и задачи организационно-правовых механизмов информационной безопасности?
3. Какие правовые нормы регулируют обеспечение информационной безопасности?
4. Что такое политика информационной безопасности и как она связана с организационно-правовыми механизмами?
5. Какие принципы должны быть учтены при разработке организационных механизмов информационной безопасности?
6. Расскажите о роли руководства организации в обеспечении информационной безопасности.
7. Какие меры по обеспечению информационной безопасности могут быть введены на уровне персонала?
8. Какие методы аутентификации и авторизации используются для защиты информации от несанкционированного доступа?
9. Какие требования предъявляются к физической безопасности информационных ресурсов?
10. Какие организационно-правовые механизмы используются для обеспечения конфиденциальности информации?
11. Расскажите о роли системы управления информационной безопасностью (СУИБ) в организационно-правовых механизмах.
12. Какие меры должны быть приняты для защиты информации при передаче через сети связи?

13. Расскажите о механизмах контроля и мониторинга информационной безопасности в организации.

14. Какие правовые нормы регулируют ответственность за нарушение информационной безопасности?

15. Какие методы реагирования на информационные инциденты входят в организационно-правовые механизмы обеспечения информационной безопасности?

Работа №2.

Тема: Технические средства защиты информации

1. Цель и содержание

Цель работы "Разработка организационных и технических мер по технической защите информации" заключается в создании системы и механизмов, которые обеспечат безопасность информации в организации или предприятии. Эта работа имеет несколько аспектов:

Организационные меры: Цель организационных мер состоит в разработке политик, процедур и правил, которые определяют, как должна быть обрабатываться и защищаться информация в организации. Включает в себя разработку политики доступа к информации, процедур управления паролями, обучение персонала по вопросам информационной безопасности и контроль соответствия сотрудников установленным правилам.

Технические меры: Цель технических мер заключается в применении технологий и инструментов для защиты информации от несанкционированного доступа, изменений или уничтожения. Примерами таких мер являются установка физических барьеров (например, замки и системы видеонаблюдения), использование антивирусных программ и брандмауэров для обнаружения и предотвращения вторжений, шифрование данных для защиты конфиденциальности и резервное копирование информации для обеспечения ее целостности.

Результатом работы по разработке организационных и технических мер по технической защите информации должна быть эффективная система, которая минимизирует угрозы безопасности информации и обеспечивает защиту конфиденциальности, целостности и доступности данных.

2. Задание

Разработайте план организационных и технических мер по технической защите информации для организации, включающий следующие этапы:

- Анализ угроз и рисков: Проведите анализ возможных угроз безопасности информации, которым подвергается ваша организация. Определите существующие риски и потенциальные последствия инцидентов.

- Разработка политики безопасности информации: Сформулируйте политику безопасности информации, которая будет служить основой для разработки всех последующих мер по технической защите. Укажите цели, принципы и правила, которые должны быть соблюдены всеми сотрудниками.

- Защита сети: Разработайте и меры для защиты сетевой инфраструктуры организации. Включите в план использование брандмауэров, систем обнаружения вторжений (Intrusion Detection System – IDS) и систем предотвращения вторжений (Intrusion Prevention System – IPS).

- Защита данных: Определите методы шифрования данных, которые будут использоваться для защиты конфиденциальной информации. Разработайте план резервного копирования данных и обеспечения их целостности.

- Управление учетными записями: Создайте стратегию управления учетными записями, включающую разграничение прав доступа, установку сложных паролей, периодическое обновление паролей и мониторинг активности пользователей.

- Физическая безопасность: Определите организационные меры для обеспечения физической защиты серверных комнат, центров обработки данных и других важных объектов. Рассмотрите использование систем видеонаблюдения, контроля доступа и ограничения зоны доступа.

- Обучение персонала: Разработайте программу обучения и осведомленности сотрудников о правилах информационной безопасности.

- Мониторинг и аудит: Разработайте процедуры для анализа журналов событий и реагирования на инциденты.

Ваша задача состоит в том, чтобы разработать подробный план с описанием каждого этапа и соответствующими мерами по технической защите информации. Обоснуйте выбор конкретных мер и инструментов на основе анализа угроз и рисков, а также целей организации в области безопасности информации.

Контрольные вопросы

1. Какие организационные меры обеспечивают техническую защиту информации?
2. Какой роль играет политика безопасности в разработке мер по технической защите информации?

3. Какими методами можно обеспечить контроль доступа к конфиденциальной информации?

4. Какие технические меры используются для защиты информации от несанкционированного доступа?

5. Что такое аутентификация и какие методы аутентификации могут быть применены для технической защиты информации?

6. Каковы основные принципы шифрования информации и какие шифровальные алгоритмы можно использовать?

7. Какие меры могут быть предприняты для предотвращения атак по перехвату данных, например, через сетевые протоколы?

8. Какие меры обеспечивают сохранность данных при их хранении и передаче?

9. Как влияют физические меры безопасности на техническую защиту информации?

10. Какие меры предусмотрены для защиты информации от вредоносного программного обеспечения (вирусы, трояны и т.д.)?

11. Каковы основные этапы разработки системы технической защиты информации?

12. Какие меры могут быть предприняты для обеспечения надежности и целостности хранения информации?

13. Какие меры предусмотрены для защиты информации от несанкционированного копирования или распространения?

14. Какова роль мониторинга и аудита в обеспечении технической защиты информации?

15. Какие требования и стандарты следует учитывать при разработке организационных и технических мер по технической защите информации?

Работа №3.

Тема: Защита персональных данных.

1. Цель и содержание

Целью защиты персональных данных является обеспечение конфиденциальности, целостности и доступности личной информации, собираемой и обрабатываемой организациями или индивидуальными лицами. Она направлена на предотвращение несанкционированного доступа к персональным данным, их утраты, повреждения или несанкционированной модификации.

Основные задачи работы по защите персональных данных:

- Соблюдение юридических требований: Работа должна быть направлена на соблюдение соответствующих законодательных норм и нормативных актов, связанных с защитой персональных данных, таких как Общий регламент по защите данных (GDPR) в Европейском союзе или Федеральный закон "О персональных данных" в Российской Федерации.

- Разработка политик и процедур: Необходимо разработать и внедрить политики и процедуры, определяющие правила сбора, использования, хранения и уничтожения персональных данных. Эти документы должны быть понятными для всех сотрудников и соответствовать юридическим требованиям.

- Обучение сотрудников: Важно провести обучение сотрудников организации по вопросам защиты персональных данных, включая правила хранения и передачи информации, а также о возможных последствиях нарушения требований по защите персональных данных.

- Разработка технических мер безопасности: Необходимо принять меры по обеспечению технической безопасности, такие как шифрование данных, установка брандмауэров и антивирусного программного обеспечения, регулярное обновление программного обеспечения и системных обновлений, контроль доступа к информации и т. д.

- Управление инцидентами: Работа по защите персональных данных должна предусматривать план действий в случае возникновения инцидентов связанных с персональными данными, таких как утечка информации или взлом системы. Необходимо иметь процедуру реагирования на такие инциденты, включая оповещение компетентных органов и клиентов, которых это затрагивает.

2. Теоретическое обоснование

Защита персональных данных имеет фундаментальное теоретическое обоснование, основанное на следующих принципах и концепциях:

- Право на личную жизнь: Каждый человек имеет право на личную жизнь и неприкосновенность своей личности. Защита персональных данных является неотъемлемой частью этого права, поскольку персональные данные могут содержать чувствительную информацию о человеке, которая может быть использована для его идентификации или вмешательства в его частную сферу.

- Информационная автономия: Защита персональных данных связана с уважением информационной автономии каждого человека. Люди должны иметь контроль над собственной информацией и иметь возможность решать, какую информацию о себе они хотят раскрывать, кому и для каких целей.

- Принцип минимизации данных: Согласно этому принципу, субъекты персональных данных должны предоставлять только необходимую информацию, которая требуется для достижения определенных целей. Обработчики данных должны собирать, обрабатывать и хранить только минимальное количество персональных данных, необходимое для выполнения определенной задачи.

- Конфиденциальность: Защита персональных данных направлена на обеспечение конфиденциальности информации, предоставленной лицами. Организации должны принимать меры для предотвращения несанкционированного доступа, использования или раскрытия персональных данных.

- Целостность и доступность данных: Защита персональных данных также включает обеспечение целостности и доступности информации. Информация должна быть защищена от случайной или злонамеренной потери, повреждения или изменения, а также должна быть доступна только авторизованным пользователям в определенных условиях.

- Соответствие законодательству: Защита персональных данных основывается на соответствии применимому законодательству в данной юрисдикции. Законы, такие как GDPR в ЕС или Федеральный закон "О персональных данных" в России, устанавливают правила и требования для сбора, обработки и хранения персональных данных.

3. Задание

Кейс-задача: Защита персональных данных для предприятия ООО ЦСБ "ЩИТ-ИНФОРМ"

Описание предприятия: ООО ЦСБ "ЩИТ-ИНФОРМ" занимается разработкой и предоставлением программного обеспечения для управления информационной безопасностью в организациях. Компания хранит и обрабатывает большое количество персональных данных своих клиентов, включая информацию о сотрудниках компаний-клиентов.

Задача: Разработка системы защиты персональных данных в соответствии с требованиями законодательства о защите персональных данных.

Шаги решения:

1. Анализ законодательства: Изучите законодательные акты, регулирующие защиту персональных данных, такие как Общий регламент ЕС о защите данных (GDPR) или Федеральный закон "О персональных данных" в России. Подробно изучите требования по обработке, хранению и передаче персональных данных.
2. Инвентаризация данных: Составьте полный список всех категорий персональных данных, которые собираются, хранятся и обрабатываются в предприятии. Укажите цель сбора каждой категории персональных данных.
3. Оценка уязвимостей: Проведите аудит информационной системы компании, чтобы выявить уязвимости в защите персональных данных. Включите проверку физической безопасности серверов, доступа к данным, шифрования и других мер защиты.
4. Разработка политики защиты персональных данных: На основе анализа законодательства и выявленных уязвимостей разработайте политику защиты персональных данных для предприятия. В политике должны быть установлены правила по обработке, хранению и передаче персональных данных, а также меры безопасности, которые необходимо применять.
5. Сообщение об инцидентах: Разработайте процедуры для обработки и уведомления о возможных нарушениях безопасности персональных данных. Обеспечьте механизмы для своевременного обнаружения и реагирования на подобные инциденты.
6. Сотрудничество с внешними экспертами: Рассмотрите возможность сотрудничества с внешними специалистами по защите персональных данных для получения дополнительной экспертизы и консультаций.

Контрольные вопросы

1. Какие личные данные считаются конфиденциальными?
2. Что такое обработка персональных данных?
3. Какую информацию можно считать персональными данными?
4. Какие меры безопасности следует принять для защиты персональных данных?
5. Какие законы и нормативные акты регулируют защиту персональных данных в вашей стране?
6. Какие права имеют пользователи в отношении своих персональных данных?
7. Что такое согласие на обработку персональных данных и почему оно важно?
8. Какие шаги можно предпринять, чтобы защитить свои персональные данные при использовании интернета?
9. Какие риски связаны с передачей персональных данных через открытые Wi-Fi сети?
10. Какие меры безопасности следует принять при работе с электронной почтой для защиты персональных данных?
11. Каким образом компании должны хранить и обрабатывать персональные данные своих клиентов?
12. Что такое двухфакторная аутентификация и как она помогает защитить персональные данные?
13. Какие шаги следует предпринять в случае утечки персональных данных или нарушения безопасности?
14. Какие меры безопасности следует принять при использовании мобильных устройств для защиты персональных данных?
15. Какие требования GDPR (Общий регламент по защите данных) накладывает на компании в отношении обработки и защиты персональных данных?

Работа №4.

Тема: Разработка организационно-распорядительной документации для объекта информатизации

1. Цель и содержание

Цель работы с организационно-распорядительной документацией в сфере информационной безопасности состоит в обеспечении защиты информации путем правильного применения и соблюдения соответствующих норм и правил. Основные задачи работы с нормативно-правовыми документами в сфере информационной безопасности включают:

- Изучение и анализ действующего законодательства и нормативных актов, регулирующих информационную безопасность. Это включает изучение международных, национальных и отраслевых стандартов, законов, постановлений, указов и других регуляторных документов.

- Интерпретация и применение норм и требований, содержащихся в нормативно-правовых документах. Работник в области информационной безопасности должен разбираться в том, какие меры необходимо предпринять для обеспечения безопасности информации, и какие требования должны быть учтены при разработке и внедрении систем и технологий.

- Разработка и внедрение политик, процедур и практик в соответствии с требованиями нормативно-правовых документов. Это включает разработку политик безопасности, стандартов, регламентов, инструкций и других документов, определяющих правила и процедуры работы с информацией.

- Обеспечение соответствия организации требованиям нормативно-правовых документов. Работник должен контролировать выполнение установленных требований и проводить аудиты для проверки соответствия системы информационной безопасности законодательству и регуляторным нормам.

- Участие в процессе разработки новых нормативно-правовых документов в области информационной безопасности. Работник может принимать активное участие в работе экспертных групп, комитетов и форумов по разработке и совершенствованию законодательства и стандартов в области информационной безопасности.

Таким образом, основная цель работы с нормативно-правовыми документами в сфере информационной безопасности заключается в обеспечении защиты конфиденциальности, целостности и доступности информации, а также защите от несанкционированного доступа, использования и распространения информации.

2. Задание

Подготовьте презентацию на тему " Разработка организационно-распорядительной документации для объекта информатизации ".

Презентация должна включать следующие пункты:

- Введение в тему: объясните, что такое нормативно-правовые документы в контексте информационной безопасности и почему они важны.

- Обзор основных законодательных и нормативных актов в области информационной безопасности, как на международном, так и национальном уровне.

- Описание процесса работы с нормативно-правовыми документами: как найти актуальные версии документов, как они структурированы и какие разделы и положения следует особо учитывать.

- Роль нормативно-правовых документов в обеспечении информационной безопасности: как они помогают предотвратить утечки данных, защитить системы от несанкционированного доступа и реагировать на инциденты.

- Примеры случаев, когда нормативно-правовые документы в сфере информационной безопасности играли важную роль и помогли предотвратить угрозы или минимизировать последствия инцидентов.

- Рекомендации по работе с нормативно-правовыми документами: какие процедуры и практики следует внедрить в организации для эффективного соблюдения требований информационной безопасности.

Презентация должна быть логически структурированной, содержать понятные иллюстрации и примеры, а также предоставлять релевантные источники информации для дальнейшего изучения темы.

Контрольные вопросы

1. Какие нормативно-правовые документы регулируют работу в сфере информационной безопасности?
2. Что такое ГОСТ Р и какую роль он играет в работе с нормативно-правовыми документами в сфере информационной безопасности?
3. Какие основные принципы работы с нормативно-правовыми документами в информационной безопасности следует учитывать?
4. Какие требования обычно предъявляются к оформлению нормативно-правовых документов в сфере информационной безопасности?
5. Какие действия должны быть предприняты в случае изменений в нормативно-правовой базе по информационной безопасности?
6. Какова роль Роскомнадзора в работе с нормативно-правовыми документами в сфере информационной безопасности?
7. Какие требования обычно предъявляются к защите персональных данных в нормативно-правовых документах?
8. Какие ответственности могут быть наложены на организации в случае нарушения нормативно-правовых требований по информационной безопасности?
9. Какие международные стандарты информационной безопасности существуют и как они связаны с российскими нормативно-правовыми документами?
10. Какие основные этапы проходит нормативно-правовой документ в процессе его разработки и принятия?
11. Какие специалисты должны быть вовлечены в работу с нормативно-правовыми документами по информационной безопасности?
12. Какие требования предъявляются к процедуре аутентификации и авторизации пользователей в нормативно-правовых документах?
13. Какие полномочия имеет Федеральная служба безопасности (ФСБ) в сфере информационной безопасности и как они отражены в нормативно-правовых документах?
14. Какие меры обеспечения информационной безопасности предусмотрены в нормативно-правовых документах для предотвращения утечек конфиденциальных данных?
15. Какие требования предъявляются к хранению и передаче информации в нормативно-правовых документах по информационной безопасности?

Работа №5.

Тема: Анализ эффективности применения средств защиты информации на объекте информатизации

Цель и содержание

Цель анализа эффективности применения средств защиты информации на объекте информатизации состоит в исследовании и оценке эффективности использования различных средств защиты информации на объекте информатизации. Объектом информатизации может быть компьютерная система, сеть, база данных или любой другой объект, содержащий ценную информацию.

Для достижения этой цели необходимо выполнить следующие задачи:

1. Изучение существующих средств защиты информации: провести обзор и анализ различных методов, технологий и программных решений, используемых для защиты информации. Оценить их преимущества и недостатки с точки зрения эффективности и применимости на конкретном объекте информатизации.

2. Анализ угроз безопасности информации: проанализировать возможные угрозы безопасности, которым подвергается объект информатизации. Рассмотреть различные виды атак, включая внешние и внутренние угрозы, и оценить их потенциальные последствия.

3. Определение требований к защите информации: определить основные требования к безопасности информации на объекте информатизации. Рассмотреть юридические, организационные и технические меры, которые должны быть применены для обеспечения надежной защиты.

4. Оценка эффективности средств защиты информации: провести анализ эффективности применяемых средств защиты информации на объекте информатизации. Сравнить результаты с требованиями безопасности и выявить возможные пробелы или слабые места в системе защиты.

5. Разработка рекомендаций по улучшению защиты информации: на основе результатов анализа предложить конкретные рекомендации по улучшению эффективности средств защиты информации на объекте информатизации. Включить в них внедрение новых технологий, обновление программного обеспечения, усиление политик безопасности и обучение персонала.

Задание

1. Изучение текущей конфигурации сетевого оборудования:

- Необходимо собрать информацию о сетевом оборудовании в предприятии "ЩИТ-ИНФОРМ", включая модели, версии прошивок и настройки.
- Необходимо проанализировать документацию и спецификации оборудования для понимания его возможностей и функциональности.

2. Анализ угроз безопасности информации:

- Провести анализ угроз безопасности, связанных с сетевой инфраструктурой предприятия "ЩИТ-ИНФОРМ".
- Рассмотреть различные виды атак, такие как DDoS-атаки, внедрение вредоносного кода, несанкционированный доступ и другие.
- Идентифицировать потенциальные уязвимости сетевого оборудования и риски, связанные с текущей конфигурацией.

3. Определение требований к безопасности информации:

- Изучить законодательные нормы, регуляторные требования и стандарты безопасности, применимые к деятельности предприятия "ЩИТ-ИНФОРМ".
- Провести консультации с заинтересованными сторонами (руководство, IT-специалисты, юристы и т. д.) для определения основных требований к безопасности информации.
- Составить список требований, включая аспекты физической, логической и организационной безопасности.

4. Составление плана улучшения защиты информации:

- На основе результатов анализа угроз и требований к безопасности, составить план мероприятий по улучшению защиты информации на предприятии "ЩИТ-ИНФОРМ".
- Включить в план такие меры, как обновление прошивок и патчей для сетевого оборудования, усиление правил фильтрации трафика, внедрение механизмов обнаружения вторжений, использование шифрования данных и другие соответствующие меры.

5. Составление отчета: Составить отчет о выполненном анализе и улучшении системы защиты информации на предприятии "ЩИТ-ИНФОРМ".

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

1. Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице 1.

Таблица 1 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 1

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

2. Вычислить все необходимые показатели угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_i + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы средняя;
- если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы высокая;
- если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;
- средняя опасность - если реализация угрозы может привести к

негативным последствиям;

- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 2.

Таблица 2 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

3. Построить модель угроз по примеру таблицы 3.

Таблица 3 - Модель угроз безопасности защищаемого объекта

Угроза	Вероятность реализации угрозы	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Несанкционированный доступ к компьютерам	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража технических средств с хранящейся в них информацией	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража носителей информации	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража материальных и финансовых ценностей	Средняя вероятность (5)	0,5 (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероятность (5)	0, 6 (средняя)	Высокая	Актуальная

Прослушивание телефонных и радиопереговоров	Средняя вероят-ность(5)	0,5 (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

1 Что подразумевается под моделью угроз безопасности информационной системы?

2 Какие основные шаги следует выполнить при составлении модели угроз безопасности информационной системы?

3 Какие типы угроз могут быть учтены при составлении модели?

4 Каким образом проводится идентификация и анализ потенциальных угроз безопасности информационной системы?

5 Какие методы и инструменты используются при составлении модели угроз безопасности информационной системы?

6 Каким образом определяются вероятность и воздействие угроз в модели безопасности информационной системы?

7 Какие факторы нужно учитывать при оценке рисков и последствий угроз безопасности информационной системы?

8 Каким образом составленная модель угроз может быть использована для планирования мер по обеспечению безопасности информационной системы?

9 Какая роль имеет обновление и поддержка модели угроз в процессе обеспечения безопасности информационной системы?

10 Какие вызовы могут возникнуть при составлении и использовании модели угроз безопасности информационной системы?

11 Какие критерии и метрики можно использовать для оценки эффективности применения средств защиты информации на объекте информатизации?

12 Какие методы и инструменты можно применить для проведения оценки эффективности средств защиты информации на объекте информатизации?

13 Какие риски и угрозы могут возникнуть при недостаточно эффективном применении средств защиты информации? Как их можно выявить и измерить?

14 Каковы основные шаги и этапы процесса оценки эффективности применения средств защиты информации на объекте информатизации?

15 Как можно оптимизировать и повысить эффективность применения средств защиты информации на объекте информатизации на основе результатов оценки?

Работа №6.
Тема: Разработка модели угроз информационной безопасности

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

4. Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице 1.

Таблица 1 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 1

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

5. Вычислить все необходимые показатели угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_i + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы средняя;
- если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы высокая;
- если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;

- средняя опасность - если реализация угрозы может привести к негативным последствиям;

- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 2.

Таблица 2 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

6. Построить модель угроз по примеру таблицы 3.

Таблица 3 - Модель угроз безопасности защищаемого объекта

Угроза	Вероят-ность реализаци и угрозы	Возмож-ность реализации угрозы	Показатель опасности угрозы	Актуаль-ность угрозы
Несанкционированный доступ к компьютерам	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража технических средств с хранящейся в них информацией	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража носителей информации	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальн ая
Кража материальных и финансовых ценностей	Средняя вероят-ность (5)	0,5 (средняя)	Высокая	Актуальная

Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероят-ность (5)	0, 6 (средняя)	Высокая	Актуальная
Прослушивание телефонных и радиопереговоров	Средняя вероят-ность(5)	0,5 (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

1. Что такое модель угроз информационной безопасности?
2. Какие основные компоненты включает модель угроз?
3. Каким образом модель угроз помогает в обеспечении информационной безопасности?
4. Какие этапы включает процесс разработки модели угроз?
5. Какие методы и подходы используются при разработке модели угроз информационной безопасности?
6. Какие типы угроз могут быть учтены в модели угроз?
7. Какие инструменты и технологии могут быть применены для разработки модели угроз информационной безопасности?
8. Какие роли могут быть назначены при разработке модели угроз?
9. Какие факторы следует учитывать при оценке уровня риска в модели угроз?
10. Какие методы анализа используются для оценки уровня угрозы в модели угроз?
11. Какая роль уязвимостей в модели угроз информационной безопасности?
12. Какие меры предосторожности можно предпринять для снижения уровня угрозы на основе модели угроз?
13. Какие преимущества имеет использование модели угроз информационной безопасности?
14. Какие ограничения могут быть связаны с применением модели угроз?
15. Какой подход может быть использован для непрерывного обновления и совершенствования модели угроз информационной безопасности?

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ, Об информации, информационных технологиях и о защите информации
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №. 55/86/20
4. Приказ ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 г. № 996 Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России от 15.02.2008 г.
7. Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 20.07.2013) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
8. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
9. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденные 13.12.2013 г. Руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
10. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности
11. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от «18» февраля 2013 г. № 21.// Официальный сайт ФСТЭК России. URL: http://fstec.ru/component/attachments/download/562 (дата обращения: 15.09.2014).

12. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности http://www.securitycode.ru/upload/iblock/8e9/algoritm-deystviy-operatora-pdn-po-sozdaniyu- si stemy-zashchity-ispdn.pdf

13. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. – URL: https://biblioclub.ru/index.php?page=book&id=611314 (дата обращения: 04.05.2023). - Режим доступа: по подписке. – Текст : электронный.

14. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – URL: https://biblioclub.ru/index.php?page=book&id=612162 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.

15. Информационная безопасность в цифровом обществе : учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.

16. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 1. - 150 с. - Текст : электронный.

17. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 2. - 303 с. - Текст : электронный.