**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
17 марта 2022 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по междисциплинарному курсу

МДК.03.01. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. Методические указания по выполнению практических работ.

Составил: Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания практических занятий, предусмотренных рабочей программой **МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**. Каждая работа рассчитана на 2 академических часа, общий объём составляет 38 часов. Нумерация рисунков, формул и таблиц в пределах одной работы. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рассмотрено и одобрено предметной (цикловой) комиссией информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля.

СОДЕРЖАНИЕ

	Наименование работы
1	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке
2	Обоснование необходимости создания подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов
3	Особенности утечки информации в проводных линиях связи
4	Особенности утечки информации в беспроводных линиях связи
5	Исследование уязвимостей и построение модели угроз объекта защиты
6	Исследование возможностей системы оценки защищенности оптических линий связи
7	Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу пэмин
8	Исследование возможностей системы оценки защищенности выделенных помещений
9	Оценка защищенности информации по акустическому каналу
10	Оценка защищенности информации по электромагнитному каналу
11	Определение каналов утечки пэмин
12	Работа с оборудованием по защите от утечки по пэмин
13	Работа с оборудованием по защите от утечки по пэмин
14	Определение утечки по цепям электропитания и заземления
15	Защита от утечки по цепям электропитания и заземления
16	Определение утечки информации по акустическому каналу
17	Работа с оборудованием по защите от утечки по акустическому каналу
18	Определение утечки информации по виброакустическому каналу
19	Работа с оборудованием по защите от утечки по виброакустическому каналу

Практическое занятие 1.

СОДЕРЖАТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ РУКОВОДЯЩИХ, НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ПРОТИВОДЕЙСТВИЮ ТЕХНИЧЕСКОЙ РАЗВЕДКЕ

1. Цель работы: ознакомиться с основными руководящими, нормативными и методическими документами, регулирующими защиту информации и противодействие технической разведке, а также научить их проводить содержательный анализ этих документов.

2. Задачи работы:

- Изучение основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.
- Определение содержания и основных положений документов.
- Оценка актуальности и эффективности документов.
- Составление аналитического отчета по результатам исследования документов.

Студент должен:

Иметь практический опыт:

- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- документы в области защиты информации.

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:

- каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Выбрать один из основных руководящих, нормативных или методических документов по защите информации и противодействию технической разведке,

изучить его содержание и основные положения, оценить его актуальность и эффективность, а затем написать аналитический отчет.

5. **Содержание отчета**
    1) название и цель работы;
    2) перечень осваиваемых компетенций;
    3) задание;
    4) исходные данные по заданию/варианту;
    5) ход выполнения работ;
    6) выводы по работе;
    7) ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
    1. Какие документы регулируют защиту информации и противодействие технической разведке?
    2. Какие основные положения содержатся в Федеральном законе "О государственной тайне"?
    3. Что такое несанкционированный доступ к информации?
    4. Какие меры защиты информации утверждены приказом ФСБ РФ?
    5. Какие методические рекомендации по защите информации разработаны ФСБ РФ?

Приложение 1

Краткие сведения из теории

Основными руководящими, нормативными и методическими документами, регулирующими защиту информации и противодействие технической разведке, являются:

- Федеральный закон "О государственной тайне"
- Федеральный закон "Об информации, информационных технологиях и о защите информации"
- Положение о федеральной службе безопасности Российской Федерации
- Нормы и правила защиты информации от несанкционированного доступа, утвержденные приказом ФСБ РФ
- Методические рекомендации по защите информации, разработанные ФСБ РФ

Практическое занятие 2.
ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОЗДАНИЯ ПОДСИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ

1. **Цель работы**: ознакомиться с необходимостью создания подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов.
2. **Задачи работы:**
   - Изучить основные понятия в области защиты информации.
   - Разобраться в нормативных и методических документах, регулирующих вопросы защиты информации.
   - Определить необходимость создания подсистемы технической защиты инфокоммуникационной системы.
   - Определить требования к подсистеме технической защиты и выбрать соответствующие средства и методы защиты.

Студент должен:
Иметь практический опыт:

- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:

- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Создать план мероприятий по созданию подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов.

5. **Порядок выполнения работы**

В плане необходимо учесть следующие этапы:

- Анализ рисков и уязвимостей инфокоммуникационной системы.

- Определение требований к подсистеме технической защиты.
- Выбор средств и методов защиты.
- Разработка технического задания на создание подсистемы технической защиты.
- Разработка проекта подсистемы технической защиты.
- Реализация подсистемы технической защиты.
- Тестирование и анализ эффективности работы подсистемы технической защиты.

6. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

- Что такое техническая защита информации?
- Какие нормативные и методические документы регулируют вопросы защиты информации?
- Что такое подсистема технической защиты?

Приложение 1

Краткие сведения из теории

Техническая защита информации – это совокупность мероприятий, направленных на защиту информации от неправомерного доступа, использования, разглашения, модификации и уничтожения. Подсистема технической защиты – это часть общей системы защиты информации, которая обеспечивает защиту технических средств, используемых для обработки, хранения и передачи информации.

Практическое занятие 3.
ОСОБЕННОСТИ УТЕЧКИ ИНФОРМАЦИИ В ПРОВОДНЫХ ЛИНИЯХ СВЯЗИ

1. **Цель работы**: изучение особенностей утечки информации в проводных линиях связи и определение методов защиты от нее.

2. **Задачи работы:**
   - Изучение принципов работы проводных линий связи.
   - Анализ основных угроз и уязвимостей проводных линий связи.
   - Изучение методов и средств обнаружения утечки информации.
   - Изучение методов и средств защиты от утечки информации.
   - Оценка эффективности применяемых методов и средств защиты от утечки информации.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Изучить способы защиты от утечки информации в проводных линиях связи и разработать план мероприятий по защите информации на конкретном объекте.

5. **Содержание отчета**
   1) название и цель работы;
   2) перечень осваиваемых компетенций;

3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1) Что такое проводные линии связи?
2) Что такое утечка информации?
3) Какие причины утечки информации в проводных линиях связи?
4) Какие методы защиты от утечки информации в проводных линиях связи вы знаете?

Приложение 1

Краткие сведения из теории

Проводные линии связи - это система передачи данных, которая использует провода или кабели для передачи сигнала от источника к приемнику. Однако, при передаче сигнала по проводам, частичка сигнала может распространиться в окружающей среде и быть перехваченной злоумышленниками. Это называется утечкой информации.

Основные причины утечки информации в проводных линиях связи включают:

- Электромагнитные излучения
- Электрические импульсы
- Неисправности в проводах
- Сигналы, проходящие через открытые окна или двери

Для защиты от утечки информации в проводных линиях связи могут использоваться следующие методы:

- Кабельная экранировка
- Использование фильтров
- Подключение устройств только через автоматические переключатели
- Криптографические методы

Практическое занятие 4.
ОСОБЕННОСТИ УТЕЧКИ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ ЛИНИЯХ СВЯЗИ

1. **Цель работы**: изучение особенностей утечки информации в беспроводных линиях связи, а также методов защиты от такой утечки.

2. **Задачи работы:**
   - Изучение принципов работы беспроводных сетей;
   - Изучение методов и инструментов для анализа и обнаружения утечек информации в беспроводных сетях;
   - Ознакомление с механизмами защиты беспроводных сетей и методами предотвращения утечек информации;
   - Практическое ознакомление с методами настройки безопасности беспроводных сетей.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

1. Настройка безопасности беспроводной сети с использованием протокола WPA2;
2. Проведение тестирования безопасности беспроводной сети при помощи инструмента Kali Linux.

5. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое беспроводные сети и как они работают?
2. Какие методы защиты используются для защиты информации в беспроводных сетях?
3. Какой протокол безопасности беспроводных сетей считается наиболее безопасным на данный момент?
4. Какие инструменты можно использовать для обнаружения утечек информации в беспроводных сетях?

Приложение 1

Краткие сведения из теории

Беспроводные сети работают на частотах, которые могут проникать через стены и препятствия, что может приводить к утечке информации. Как правило, протоколы безопасности беспроводных сетей используют шифрование для защиты информации. Протокол WPA2 считается наиболее безопасным на данный момент.

Практическое занятие 5.
ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ И ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ ОБЪЕКТА ЗАЩИТЫ

1. **Цель работы**: изучение методов и технологий исследования уязвимостей объектов защиты и построение модели угроз, которые могут возникнуть при использовании различных информационных систем.
2. **Задачи работы:**
   - Изучение основных методов исследования уязвимостей объектов защиты.
   - Освоение современных инструментов для обнаружения и анализа уязвимостей.
   - Изучение методов и технологий построения моделей угроз и определение вероятности их реализации.
   - Осуществление практических заданий по исследованию уязвимостей и построению моделей угроз.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Проведение исследования уязвимостей на локальной сети с использованием специализированных инструментов и построение модели угроз для данной сети.

5. **Содержание отчета**

1) название и цель работы;

2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое исследование уязвимостей?
2. Какие инструменты используются для обнаружения уязвимостей?
3. Что такое модель угроз?
4. Какие преимущества даёт моделирование угроз при проектировании информационных систем?
5. Каким образом можно снизить риск возникновения угроз?

Приложение 1

Краткие сведения из теории

Исследование уязвимостей – это процесс определения слабых мест в информационных системах, сетях и приложениях, которые могут быть использованы злоумышленниками для получения несанкционированного доступа или нарушения работы системы.

Модель угроз – это описание потенциальных угроз, которые могут возникнуть при использовании определенной информационной системы или технологии. Она позволяет оценить вероятность реализации каждой угрозы и принять меры по устранению или снижению рисков.

Практическое занятие 6.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СИСТЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

1. Цель работы: изучение возможностей системы оценки защищенности оптических линий связи.

2. Задачи работы:

- Изучить основные методы оценки защищенности оптических линий связи.
- Изучить систему оценки защищенности оптических линий связи.
- Изучить средства защиты оптических линий связи.
- Провести исследование возможностей системы оценки защищенности оптических линий связи.

Студент должен:

Иметь практический опыт:

- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;

ПК:

- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Провести оценку защищенности оптической линии связи на основе имеющейся системы оценки и сделать рекомендации по улучшению ее защищенности.

5. Содержание отчета

1) название и цель работы;

2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое оптические линии связи?
2. Какие методы используются для оценки защищенности оптических линий связи?
3. Что такое система оценки защищенности оптических линий связи?
4. Какие средства защиты могут быть применены для оптических линий связи?

Приложение 1

Краткие сведения из теории

Оптические линии связи являются одним из наиболее надежных и безопасных способов передачи информации, однако они также могут быть подвержены различным атакам и уязвимостям. Для оценки защищенности оптических линий связи используются различные методы, такие как анализ качества передачи данных, анализ уровня шума и т.д. Системы оценки защищенности оптических линий связи позволяют оперативно выявлять уязвимости и принимать меры по их устранению.

Практическое занятие 7.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СИСТЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛУ ПЭМИН

1. **Цель работы**: изучение возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.
2. **Задачи работы:**
   - Ознакомление со стандартами и методиками оценки защищенности технических средств от утечки информации по каналу ПЭМИН.
   - Изучение принципов работы системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.
   - Практическое исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

   Протестировать систему оценки защищенности технических средств от утечки информации по каналу ПЭМИН на конкретном техническом средстве.

5. **Порядок выполнения работы**

   Для этого необходимо провести исследование утечки информации по каналу ПЭМИН, а затем применить систему оценки защищенности для оценки уровня защиты технического средства от этой утечки.

6. **Содержание отчета**

   1) название и цель работы;
   2) перечень осваиваемых компетенций;
   3) задание;
   4) исходные данные по заданию/варианту;
   5) ход выполнения работ;
   6) выводы по работе;
   7) ответы на контрольные вопросы.

7. **Контрольные вопросы к защите**

   1. Что такое система оценки защищенности технических средств от утечки информации по каналу ПЭМИН?
   2. Какие принципы лежат в основе работы системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН?
   3. Как проводится оценка уровня защиты технических средств от утечки информации по каналу ПЭМИН?

Приложение 1

Краткие сведения из теории

Система оценки защищенности технических средств от утечки информации по каналу ПЭМИН позволяет оценить уровень защищенности технических средств от утечки информации по каналу электромагнитного излучения. Оценка защищенности осуществляется на основе анализа параметров электромагнитного излучения, генерируемого техническим средством.

Практическое занятие 8.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СИСТЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ

1. **Цель работы**: ознакомиться с основами оценки защищенности выделенных помещений и возможностями соответствующих систем.

2. **Задачи работы:**
   - Изучение основных понятий и принципов системы оценки защищенности выделенных помещений.
   - Ознакомление с методами и инструментами, используемыми для оценки защищенности выделенных помещений.
   - Практическое применение полученных знаний на конкретных примерах.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

провести оценку защищенности выделенного помещения с использованием соответствующих методов и инструментов. Определить уровень защищенности помещения и предложить меры по улучшению защиты.

5. **Содержание отчета**
   1) название и цель работы;
   2) перечень осваиваемых компетенций;

3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое система оценки защищенности выделенных помещений?
2. Какие методы используются для оценки защищенности помещения?
3. Какие факторы учитываются при оценке защищенности помещения?
4. Какие меры могут быть приняты для улучшения защиты выделенных помещений?

Приложение 1

Краткие сведения из теории

Система оценки защищенности выделенных помещений представляет собой комплекс методов, инструментов и процедур, которые позволяют оценить уровень защищенности помещения от различных угроз. Оценка проводится на основе анализа физических, технических и организационных мер защиты. Для проведения оценки защищенности помещения используются различные методы, такие как анализ угроз, идентификация уязвимостей, оценка рисков и другие.

Практическое занятие 9.
ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: изучить методы оценки защищенности информации по акустическому каналу и определить меры по усилению защиты информации.
2. **Задачи работы:**
   - Изучить теоретические основы акустической защиты информации.
   - Изучить методы оценки защищенности информации по акустическому каналу.
   - Определить меры по усилению защиты информации по акустическому каналу.
   - Практически применить полученные знания для оценки защищенности информации по акустическому каналу на конкретном примере.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Изучить определенный пример использования акустической защиты информации и оценить его эффективность. Например, методы защиты информации в системах речевого управления, которые используют голосовые команды. Провести эксперименты, попробовав повлиять на работу такой системы с помощью разных типов шума, записывая и анализируя результаты.

5. **Содержание отчета**
    1) название и цель работы;
    2) перечень осваиваемых компетенций;
    3) задание;
    4) исходные данные по заданию/варианту;
    5) ход выполнения работ;
    6) выводы по работе;
    7) ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
    1. Что такое акустическая защита информации?
    2. Какие методы защиты информации по акустическому каналу существуют?
    3. Как можно провести эксперимент по оценке эффективности акустической защиты информации?
    4. Какие меры по усилению защиты информации по акустическому каналу могут быть предприняты?

Приложение 1

Краткие сведения из теории

Акустическая защита информации является одним из методов защиты информации от несанкционированного доступа. Она основывается на том, что звуковые сигналы, передаваемые по каналу связи, могут быть перехвачены и преобразованы в электрический сигнал. Чтобы предотвратить это, используются различные методы защиты, такие как шумовые генераторы и устройства защиты от записи.

Практическое занятие 10.
ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ

1. **Цель работы**: изучить методы оценки защищенности информации по электромагнитному каналу и способы защиты от утечки данных.
2. **Задачи работы:**
   - изучить принципы работы электромагнитных каналов связи;
   - изучить основные методы атак на электромагнитные каналы связи;
   - изучить методы оценки защищенности информации по электромагнитному каналу;
   - изучить методы защиты информации по электромагнитному каналу.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Разработать сценарий атаки на информационную систему по электромагнитному каналу и предложить способы защиты от такой атаки.

5. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое электромагнитный канал связи?
2. Какие методы атак на электромагнитный канал связи вы знаете?
3. Какие методы оценки защищенности информации по электромагнитному каналу вы знаете?
4. Какие методы защиты информации по электромагнитному каналу вы знаете?

Приложение 1

Краткие сведения из теории

Электромагнитный канал связи является одним из наиболее распространенных каналов передачи данных. При этом, электромагнитные излучения могут использоваться злоумышленниками для несанкционированного доступа к информации. Основные методы атак на электромагнитные каналы связи включают анализ электромагнитных излучений и генерацию электромагнитных помех. Для оценки защищенности информации по электромагнитному каналу используются методы анализа электромагнитных излучений и методы анализа радиочастотной спектральной характеристики. Основные методы защиты информации по электромагнитному каналу включают использование защитных экранов, криптографических методов и методов фильтрации шума.

Практическое занятие 11.
ОПРЕДЕЛЕНИЕ КАНАЛОВ УТЕЧКИ ПЭМИН

1. Цель работы: ознакомиться с концепцией каналов утечки ПЭМИН, научить определять каналы утечки в информационной системе и применять соответствующие меры защиты для предотвращения утечек.

2. Задачи работы:

- Изучить основные понятия, связанные с каналами утечки ПЭМИН.
- Определить каналы утечки ПЭМИН в информационной системе.
- Применить меры защиты для предотвращения утечек через каналы ПЭМИН.

Студент должен:

Иметь практический опыт:

- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:

- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Определение каналов утечки ПЭМИН в локальной сети.

5. Порядок выполнения работы

1. Подготовка:
   - Установка и настройка утилиты для анализа сетевого трафика, например, WireShark.
   - Запуск утилиты в режиме "прослушивания" сетевого трафика на нужном интерфейсе сетевой карты.
2. Анализ сетевого трафика:
   - Запустите процесс обмена информацией в локальной сети, например, отправьте запрос на доступ к ресурсу или выполните какое-либо действие в системе.
   - Анализируйте сетевой трафик, полученный в WireShark, и ищите необычные пакеты данных, которые могут свидетельствовать о возможных каналах утечки ПЭМИН.
3. Определение каналов утечки:
   - Изучите полученные данные и определите каналы утечки ПЭМИН.
   - Проанализируйте источник и природу утечки, чтобы убедиться, что она действительно является каналом утечки ПЭМИН.
4. Применение мер защиты:
   - Разработайте и примените меры защиты, чтобы предотвратить утечки через эти каналы, например, защитите уязвимые участки кода, используйте шифрование или регулярно обновляйте систему.
5. Тестирование:
   - Проверьте, работают ли примененные меры защиты.
   - Повторите анализ сетевого трафика, чтобы убедиться, что утечки информации не происходит.
   - Документирование результатов:
   - Зафиксируйте результаты анализа и применения мер защиты.
   - Документируйте все обнаруженные каналы утечки ПЭМИН и примененные меры защиты.

Важно помнить, что определение каналов утечки ПЭМИН — это сложный процесс, требующий специализированных знаний и навыков, а также использования специальных инструментов и оборудования.

6. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое каналы утечки ПЭМИН?
2. Какие аппаратные и программные средства могут быть источниками каналов утечки ПЭМИН?
3. Каким образом можно определить каналы утечки ПЭМИН?
4. Какие меры защиты могут быть применены для предотвращения утечек через каналы ПЭМИН?
5. Какие последствия могут возникнуть в случае утечки конфиденциальной информации через каналы ПЭМИН?

Приложение 1

Краткие сведения из теории

Каналы утечки ПЭМИН - это пути, по которым может происходить несанкционированное раскрытие информации, используя возможности оборудования, принципы работы программного обеспечения и технологии передачи данных. Каналы утечки ПЭМИН могут быть связаны с различными типами аппаратных и программных средств, такими как процессоры, оперативная память, жесткие диски, шины данных, программное обеспечение и т.д.

Практическое занятие 12.
РАБОТА С ОБОРУДОВАНИЕМ ПО ЗАЩИТЕ ОТ УТЕЧКИ ПО ПЭМИН

1. Цель работы: ознакомиться с оборудованием и мерами защиты от утечки по ПЭМИН и научить работать с этим оборудованием.

2. Задачи работы:

- ознакомление студентов с понятием ПЭМИН и способами защиты от утечки;
- представление оборудования для защиты от утечки по ПЭМИН;
- обучение студентов работе с оборудованием для защиты от утечки по ПЭМИН.

Студент должен:

Иметь практический опыт:

- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:

- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

   Настройка и проверка работы защиты от утечки по ПЭМИН на оборудовании. Необходимо настроить оборудование (шлюз и маршрутизатор) для защиты от утечки по ПЭМИН. Затем отправить запросы через этот оборудование и проверить, что защита от утечки по ПЭМИН работает корректно.

5. **Содержание отчета**
   1) название и цель работы;
   2) перечень осваиваемых компетенций;
   3) задание;
   4) исходные данные по заданию/варианту;
   5) ход выполнения работ;
   6) выводы по работе;
   7) ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
   1. Что такое ПЭМИН?
   2. Какие меры защиты от утечки по ПЭМИН существуют?
   3. Какие устройства используются для защиты от утечки по ПЭМИН?
   4. Что такое экранирование системы?
   5. Какие компоненты системы являются наиболее уязвимыми для утечки по ПЭМИН?

Приложение 1

Краткие сведения из теории

ПЭМИН (побочные электромагнитные излучения и наводки) - это явление, при котором электромагнитные поля, создаваемые электронными компонентами, могут вызывать утечку информации из системы. Для защиты от утечки по ПЭМИН используются различные меры, такие как:

- физическая изоляция системы;
- экранирование системы;
- защита уязвимых компонентов;
- использование криптографии.

Оборудование для защиты от утечки по ПЭМИН может включать в себя шлюзы и маршрутизаторы, а также специализированные устройства, такие как защищенные кабели и экранированные корпуса.

Практическое занятие 13.
РАБОТА С ОБОРУДОВАНИЕМ ПО ЗАЩИТЕ ОТ УТЕЧКИ ПО ПЭМИН

1. Цель работы: ознакомление с оборудованием для защиты от утечки по ПЭМИН и получение практических навыков работы с ним.

2. Задачи работы:

- Изучение принципов работы оборудования для защиты от утечки по ПЭМИН.
- Ознакомление со способами установки и настройки оборудования.
- Получение практических навыков работы с оборудованием для защиты от утечки по ПЭМИН.

Студент должен:

Иметь практический опыт:

- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;

Знать:

- основные типы технических средств защиты информации от утечки по техническим каналам;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;

ПК:

- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Настроить оборудование для защиты от утечки по ПЭМИН и проверить его работоспособность на тестовой локальной сети.

5. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое ПЭМИН?
2. Какое оборудование используется для защиты от утечки по ПЭМИН?
3. Какие функции может выполнять оборудование для защиты от утечки по ПЭМИН?
4. Какие меры безопасности необходимо предпринять при работе с оборудованием для защиты от утечки по ПЭМИН?

Приложение 1

Краткие сведения из теории

ПЭМИН (промышленные электромагнитные помехи) могут привести к утечке конфиденциальной информации из локальной сети. Для защиты от утечки по ПЭМИН существует специальное оборудование, которое блокирует возможность сбора и анализа электромагнитных излучений.

Оборудование для защиты от утечки по ПЭМИН может иметь различные форм-факторы и функции. Оно может быть предназначено для защиты от утечки только на определенной частоте, или же для общей защиты от ПЭМИН.

Практическое занятие 14.
ОПРЕДЕЛЕНИЕ УТЕЧКИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ И ЗАЗЕМЛЕНИЯ

1. **Цель работы**: ознакомление с методами определения утечки по цепям электропитания и заземлению и развитие навыков работы с необходимым оборудованием.
2. **Задачи работы:**
   - изучение принципов работы оборудования для определения утечки по цепям электропитания и заземлению;
   - ознакомление с методиками и приборами для измерения утечки по цепям электропитания и заземлению;
   - проведение практических занятий по определению утечки по цепям электропитания и заземлению на практике;
   - анализ результатов и обсуждение возможных мер по предотвращению утечек.

Студент должен:
Иметь практический опыт:

- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;

ПК:

- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Провести измерение утечки по цепям электропитания и заземлению с помощью прибора для измерения тока утечки.

5. **Содержание отчета**

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое утечка по цепям электропитания и заземлению?
2. Какие методы измерения утечки существуют?
3. Какие меры могут быть приняты для предотвращения утечки по цепям электропитания и заземлению?

Приложение 1

Краткие сведения из теории

Утечка по цепям электропитания и заземлению возникает при наличии неправильной или неисправной электрической проводки, а также при несоблюдении правил эксплуатации оборудования. Измерение утечки проводится с помощью специальных приборов, которые позволяют определить ток утечки.

Практическое занятие 15.
ЗАЩИТА ОТ УТЕЧКИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ И ЗАЗЕМЛЕНИЯ

1. Цель работы: ознакомление с методами защиты информационно-телекоммуникационных систем и сетей от утечки по цепям электропитания и заземлению.
Задачи работы:

- Изучение принципов защиты от утечки по цепям электропитания и заземлению.
- Ознакомление с основными видами электромагнитных помех и методами их снижения.
- Изучение методов защиты оборудования и систем от перенапряжений.
- Практическое ознакомление с оборудованием и программными средствами, используемыми для защиты от утечки по цепям электропитания и заземлению

Студент должен:
Иметь практический опыт:

- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;

ПК:

- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

подключение оборудования к заземлению и проведение проверки на наличие утечки по цепям электропитания..

5. Содержание отчета

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое утечка по цепям электропитания и заземлению?
2. Какие методы защиты от утечки по цепям электропитания и заземлению существуют?
3. Что такое электромагнитные помехи и какие методы снижения их уровня существуют?
4. Что такое перенапряжения и какие методы защиты от них существуют?

Приложение 1

Краткие сведения из теории

Утечка по цепям электропитания и заземлению возникает при наличии неправильной или неисправной электрической проводки, а также при несоблюдении правил эксплуатации оборудования. Измерение утечки проводится с помощью специальных приборов, которые позволяют определить ток утечки. Утечка по цепям электропитания и заземлению может возникнуть при наличии некорректного подключения или наличия неполадок в оборудовании и системах. Для защиты от таких утечек используются методы заземления, использование фильтров и стабилизаторов напряжения, а также защитные устройства от перенапряжений.

Практическое занятие 16.
ОПРЕДЕЛЕНИЕ УТЕЧКИ ИНФОРМАЦИИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: ознакомиться с проблемой утечки информации через виброакустический канал, методами определения такой утечки и способами её предотвращения.
2. **Задачи работы:**
   - Изучить теоретические основы виброакустической утечки информации.
   - Изучить методы определения утечки информации через виброакустический канал.
   - Освоить способы защиты от виброакустической утечки информации.
   - Практическое освоение методов и способов защиты от утечки информации через виброакустический канал.

Студент должен:

Иметь практический опыт:

- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;

ПК:

- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

провести эксперимент, направленный на определение возможности утечки информации через виброакустический канал.

5. **Порядок выполнения работы**

Для этого нужно включить микрофон на смартфоне, набрать на другом телефоне цифры и поочередно прижимать его к различным поверхностям (стол, стена, дверь и т.д.). Затем проанализировать запись звука и определить, какие звуки могут свидетельствовать о возможной утечке информации. **Содержание отчета**

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**

1. Что такое виброакустическая утечка информации?
2. Какие устройства можно использовать для осуществления виброакустической атаки?
3. Какие методы защиты от виброакустической утечки информации существуют?

Приложение 1

Краткие сведения из теории

Виброакустическая утечка информации – это метод получения информации путем измерения механических вибраций, создаваемых объектом, на который направлена атака. Вибрации могут возникать при нажатии клавиш на клавиатуре, при разговоре по телефону, а также при передаче данных по сети. Эти вибрации могут быть замерены и использованы для извлечения информации.

Практическое занятие 17.
РАБОТА С ОБОРУДОВАНИЕМ ПО ЗАЩИТЕ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: научиться работать с оборудованием по защите от утечки по акустическому каналу и применять соответствующие технические меры для защиты информации.

2. **Задачи работы:**
   - Изучить принципы работы и настройки оборудования по защите от утечки по акустическому каналу.
   - Определить каналы утечки по акустическому каналу в локальной сети.
   - Применить соответствующие технические меры для защиты информации от утечки по акустическому каналу.
   - Оценить эффективность применяемых мер защиты.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**
- Настроить оборудование по защите от утечки по акустическому каналу.
- С использованием специальных программ определить каналы утечки по акустическому каналу в локальной сети.
- Применить соответствующие технические меры для защиты информации от утечки по акустическому каналу.

- Проверить эффективность применяемых мер защиты.

5. Порядок выполнения работы

- Изучить теоретические основы работы с оборудованием по защите от утечки по акустическому каналу.
- Настроить оборудование в соответствии с его инструкцией.
- С использованием специальных программ определить каналы утечки по акустическому каналу в локальной сети.
- Применить соответствующие технические меры для защиты информации от утечки по акустическому каналу.
- Проверить эффективность применяемых мер защиты.

6. Оценить результаты выполненной работы и подготовить отчет. **Содержание отчета**

1) название и цель работы;
2) перечень осваиваемых компетенций;
3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;

Приложение 1

Краткие сведения из теории

Утечка информации по акустическому каналу возникает, когда звуковые волны, которые генерируются при работе компьютера или других устройств, могут быть использованы для извлечения конфиденциальной информации. Для защиты от утечки по акустическому каналу используются различные технические меры, включая использование звукопоглощающих материалов, шумоподавляющих устройств, шифрования звука и друг

Практическое занятие 18.
ОПРЕДЕЛЕНИЕ УТЕЧКИ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: научиться определять утечку информации по виброакустическому каналу и использовать средства защиты от такой утечки.

2. **Задачи работы:**
   - Изучение теории и принципов работы виброакустического канала и возможных методов атаки на него.
   - Определение утечки информации по виброакустическому каналу на модельной системе.
   - Определение эффективности средств защиты от утечки информации по виброакустическому каналу.
   - Разработка рекомендаций по улучшению защиты от утечки информации по виброакустическому каналу.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

1. Подготовить экспериментальную модель системы, содержащей информацию, которую нужно защитить от утечки по виброакустическому каналу.
2. Провести тестирование утечки информации по виброакустическому каналу с использованием специального оборудования.

3. Протестировать эффективность различных средств защиты от утечки информации по виброакустическому каналу, таких как виброзащита, звукопоглощающие материалы и шумогенераторы.
4. Проанализировать результаты и сделать выводы о наиболее эффективных методах защиты от утечки информации по виброакустическому каналу.

5. Порядок выполнения работы

- Изучение теории и принципов работы виброакустического канала.
- Подготовка экспериментальной модели системы с информацией, которую нужно защитить от утечки по виброакустическому каналу.
- Тестирование утечки информации по виброакустическому каналу с использованием специального оборудования.
- Тестирование эффективности средств защиты от утечки информации по виброакустическому каналу.
- Анализ результатов и написание отчета.

6. Содержание отчета
    1) название и цель работы;
    2) перечень осваиваемых компетенций;
    3) задание;
    4) исходные данные по заданию/варианту;
    5) ход выполнения работ;
    6) выводы по работе;
    7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое виброакустический канал передачи информации?
2. Каким образом может происходить утечка информации по виброакустическому каналу?
3. Какие методы могут использоваться для определения утечки информации по виброакустическому каналу?
4. Какие измерительные приборы могут использоваться для определения утечки информации по виброакустическому каналу?
5. Каким образом можно предотвратить утечку информации по виброакустическому каналу?

Приложение 1

Краткие сведения из теории

Виброакустический канал - это канал передачи информации посредством вибрации твердых тел, таких как стены, окна или двери. Атакующие могут использовать специальное оборудование для прослушивани

Практическое занятие 19.
РАБОТА С ОБОРУДОВАНИЕМ ПО ЗАЩИТЕ ОТ УТЕЧКИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: изучить методы защиты от утечки информации по виброакустическому каналу и научиться работать с соответствующим оборудованием.

2. **Задачи работы:**
   - Изучить основы виброакустической теории и ее применение в утечке информации.
   - Ознакомиться с оборудованием, предназначенным для защиты от утечки информации по виброакустическому каналу.
   - Провести практические занятия по работе с оборудованием и осуществлению защиты от утечки информации.
   - Проанализировать результаты работы оборудования.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

На практике определить возможность утечки информации по виброакустическому каналу и использовать оборудование для ее защиты.

5. **Содержание отчета**
   1) название и цель работы;
   2) перечень осваиваемых компетенций;

3) задание;
4) исходные данные по заданию/варианту;
5) ход выполнения работ;
6) выводы по работе;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое виброакустический канал?
2. Какую информацию можно передавать через виброакустический канал?
3. Какие материалы могут быть использованы для передачи информации через виброакустический канал?

Приложение 1

Краткие сведения из теории

Виброакустический канал – это канал передачи информации, основанный на изменении звукового давления в материалах и конструкциях. Вибрация на поверхности материала создает звуковые волны, которые могут быть приняты и интерпретированы как информация. При этом информация может передаваться через материалы различной толщины и жесткости, в том числе через стены, потолки, полы и другие конструкции.