**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: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ О.В. Колбанева
21 апреля 2021 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ 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
2021

СОДЕРЖАНИЕ

	Наименование работы
1	Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации
2	Поиск и локализация скрытых видеокамер
3	Исследование методов защиты сотовых телефонов от несанкционированного прослушивания
4	Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов
5	Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора
6	Инженерно-техническая защита информации
7	Выявление и фиксация следов противоправной деятельности, связанной с использованием компьютерной деятельности
8	Исследование уровня побочного электромагнитного излучения пк
9	Снятие диаграммы направленного микрофона
10	Исследование спектра речевого сигнала
11	Определение уровня побочного излучения в канале электросвязи
12	Определение уровня побочного излучения в канале виброакустики
13	Измерение уровня маскирующего виброакустического шума
14	Измерение уровня маскирующего цифрового шума
15	Испытание учебной аудитории на утечку информации по каналу пэмин
16	Испытание учебной аудитории на утечку информации по виброакустическому каналу

Лабораторная работа 1.
ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ, ЛОКАЛИЗАЦИИ И НЕЙТРАЛИЗАЦИИ РАДИОИЗЛУЧАЮЩИХ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

1. Цель работы: ознакомление с техническими средствами обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.

2. Задачи работы:

- Изучить основные принципы работы технических средств обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.
- Ознакомиться с техническими характеристиками и принципами работы различных типов оборудования для обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.
- Получить практические навыки работы с техническими средствами обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.

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;

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;

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 и порядок выполнения работы

- Изучите основные характеристики оборудования, используемого для обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.
- Ознакомьтесь с характеристиками оборудования для обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.
- Освойте навыки работы с оборудованием, включая спектроанализаторы и анализаторы сигналов.
- Используя оборудование, проведите эксперименты по обнаружению скрытых устройств в заданной локации и определите их местоположение.

- Изучите методы нейтрализации радиоизлучающих специальных технических средств негласного получения информации

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**

- Что такое технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации?
- Какие виды технических средств используются для обнаружения радиоизлучающих устройств?
- Какие методы используются для локализации радиоизлучающих устройств?
- Что такое нейтрализация радиоизлучающих устройств и какие методы ее реализации существуют?
- Какие возможные применения имеют технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации?
- Какими способами можно защититься от обнаружения и негласного получения информации при помощи радиоизлучающих устройств?

Приложение 1

Краткие сведения из теории

Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации предназначены для выявления, определения местоположения и блокировки работы различных типов скрытых устройств, которые могут использоваться для негласного получения информации. Это может быть различное оборудование, такое как скрытые микрофоны, видеокамеры, GPS-трекеры, беспроводные передатчики и т.д. Для выполнения задачи по обнаружению, локализации и нейтрализации таких устройств используются различные типы оборудования, такие как спектроанализаторы, анализаторы сигналов, детекторы беспроводных сигналов, антенны для локализации и т.д.

Лабораторная работа 2.
ПОИСК И ЛОКАЛИЗАЦИЯ СКРЫТЫХ ВИДЕОКАМЕР

1. **Цель работы**: научиться использовать технические средства для поиска и локализации скрытых видеокамер.

2. **Задачи работы:**
   - Изучить теоретические основы работы скрытых видеокамер и методов их обнаружения.
   - Ознакомиться с техническими средствами для поиска скрытых видеокамер.
   - Практически научиться искать и локализовывать скрытые видеокамеры.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- 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;

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 и порядок выполнения работы:**
   - Изучить теоретические основы работы скрытых видеокамер и методов их обнаружения.
   - Ознакомиться с техническими средствами для поиска скрытых видеокамер.
   - Изучить теоретические основы работы скрытых видеокамер и методов их обнаружения.
     - Ознакомиться с различными типами скрытых видеокамер, их принципом работы и возможными местами установки.
     - Изучить методы поиска скрытых видеокамер, включая визуальный, акустический и радиочастотный.
   - Ознакомиться с техническими средствами для поиска скрытых видеокамер.
     - Изучить различные типы оборудования для обнаружения скрытых видеокамер, такие как инфракрасные сканеры, радиочастотные детекторы и т.д.
     - Ознакомиться с особенностями работы каждого из этих типов оборудования и их применения.
   - Изучить примеры использования скрытых видеокамер в различных сферах, таких как безопасность, разведка и т.д.
   - Провести исследование оборудования и технологий, используемых в профессиональных службах безопасности для поиска и локализации скрытых видеокамер.

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**
    - Какие методы используются для скрытия видеокамеры?
    - Какие признаки могут указывать на наличие скрытой видеокамеры?
    - Какие технические средства используются для поиска скрытых видеокамер?
    - Какие основные методы локализации скрытых видеокамер существуют?
    - Какие факторы могут повлиять на точность локализации скрытых видеокамер?
    - Какие меры безопасности следует принимать при поиске скрытых видеокамер?
    - Какие ограничения могут быть связаны с использованием технических средств поиска и локализации скрытых видеокамер?

Приложение 1

Краткие сведения из теории

Скрытые видеокамеры могут использоваться для незаконного сбора информации о людях или местах. Чтобы обнаружить скрытые камеры, можно использовать различные технические средства.

Одним из таких средств является детектор скрытых камер, который работает на основе обнаружения электромагнитных сигналов, испускаемых камерами. Другой метод - использование инфракрасных сканеров, которые могут обнаруживать тепловые излучения от скрытых камер. Также возможен поиск с помощью радиоволновых детекторов, которые могут обнаруживать сигналы, передаваемые камерами по беспроводной связи.

Для локализации скрытых камер можно использовать оптические приборы, например, зеркала с расширенным углом обзора или эндоскопы, которые позволяют просматривать труднодоступные места.

Важно отметить, что поиск скрытых камер может быть незаконным в некоторых странах и ситуациях. Поэтому перед использованием технических средств необходимо убедиться в законности проводимых действий.

Лабораторная работа 3.
ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ СОТОВЫХ ТЕЛЕФОНОВ ОТ НЕСАНКЦИОНИРОВАННОГО ПРОСЛУШИВАНИЯ

1. **Цель работы**: ознакомиться с основными методами защиты сотовых телефонов от несанкционированного прослушивания и обеспечить понимание рисков, связанных с безопасностью мобильных устройств.

2. **Задачи работы:**
   - Рассмотреть основные методы несанкционированного доступа к мобильным устройствам.
   - Ознакомиться с методами защиты мобильных устройств от несанкционированного доступа.
   - Продемонстрировать практическое применение методов 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;
- 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;

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 и порядок выполнения работы**
   - Найти и установить на смартфон приложение для защиты от взлома.
   - Настроить автоматическое шифрование всех передаваемых данных на устройстве.
   - Попробовать произвести вход на свой смартфон с помощью отпечатка пальца.

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 несанкционированное прослушивание и как оно происходит на сотовых телефонах?
2. Какие методы защиты сотовых телефонов от несанкционированного доступа существуют?
3. Какие программы можно использовать для защиты сотовых телефонов от несанкционированного доступа?

Приложение 1

Краткие сведения из теории

Сотовые телефоны являются ценными источниками информации для злоумышленников. Несанкционированное прослушивание может происходить как через прослушивание радиоканала, так и через уязвимости в программном обеспечении устройства. Для защиты мобильных устройств от несанкционированного доступа используются методы шифрования данных, парольной защиты и использования VPN-соединений.

Лабораторная работа 4.
ИССЛЕДОВАНИЕ МЕТОДОВ БЛОКИРОВАНИЯ СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО ПРОСЛУШИВАНИЯ И ПЕРЕДАЧИ ДАННЫХ РАЗЛИЧНЫХ СТАНДАРТОВ

1. **Цель работы**: изучение методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов

2. **Задачи работы:**
   - изучение средств несанкционированного прослушивания и передачи данных;
   - изучение методов блокирования средств несанкционированного прослушивания и передачи данных;
   - практическое применение методов блокирования.

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

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;

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;
- 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 и порядок выполнения работы**

Провести исследование средств несанкционированного прослушивания и передачи данных, выбрать один из стандартов (например, Wi-Fi, Bluetooth), изучить методы блокирования средств несанкционированного прослушивания и передачи данных для выбранного стандарта, а также попытаться применить эти методы на практике.

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

- Что такое средства несанкционированного прослушивания и передачи данных?
- Какие методы блокирования существуют для защиты от несанкционированного прослушивания и передачи данных?
- Какие стандарты могут быть использованы для передачи данных, и какие методы блокирования могут быть использованы для каждого из этих стандартов?

Приложение 1

Краткие сведения из теории

Средства несанкционированного прослушивания и передачи данных могут использоваться злоумышленниками для получения доступа к конфиденциальной информации. Для защиты от таких угроз существуют методы блокирования, включая использование шифрования данных, защиту паролем, фильтрацию данных и т.д.

Лабораторная работа 5.
ПОИСК УСТРОЙСТВ НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ С ПОМОЩЬЮ ПРОФЕССИОНАЛЬНОГО НЕЛИНЕЙНОГО РАДИОЛОКАТОРА

1. **Цель работы**: познакомиться с методами поиска устройств негласного съема информации и возможностью применения профессионального нелинейного радиолокатора для обнаружения таких устройств.

2. **Задачи работы:**
   - рассмотреть основные методы негласного съема информации;
   - описать принцип работы профессионального нелинейного радиолокатора;
   - обучить студентов применять профессиональный нелинейный радиолокатор для поиска устройств негласного съема информации.

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;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;

Знать:
- 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**

Использовать профессиональный нелинейный радиолокатор для поиска устройств негласного съема информации в помещении.

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.

7. Контрольные вопросы к защите

- Что такое устройства негласного съема информации?
- Как работает профессиональный нелинейный радиолокатор?
- Какие устройства можно обнаружить при помощи профессионального нелинейного радиолокатора?

Приложение 1

Краткие сведения из теории

Устройства негласного съема информации используются для несанкционированного получения информации. Такие устройства могут быть различными: микрофоны, камеры, GPS-трекеры и др. Для поиска таких устройств можно использовать профессиональный нелинейный радиолокатор. Он использует принцип работы субгармонической смеси, что позволяет обнаруживать устройства, работающие на любых частотах, включая цифровые.

Лабораторная работа 6.
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

1. Цель работы: познакомиться с основами инженерно-технической защиты информации и методами защиты информационных систем.

2. Задачи работы:

- Изучить основы инженерно-технической защиты информации;
- Рассмотреть методы защиты информационных систем;
- Определить принципы построения системы защиты информации.

Студент должен:

Иметь практический опыт:

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

Уметь:

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

Знать:

- 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;

ПК:

- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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.

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание и порядок выполнения работы

1. Изучить конструкцию и принцип работы шифровальных устройств;
2. Определить уровень утечки информации в информационной системе и разработать план мероприятий по ее защите;
3. Разработать проект защиты информационной системы на основе инженерно-технических средств.

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

- Что такое инженерно-техническая защита информации и какие ее цели?
- Какие методы защиты информационных систем существуют?
- Как происходит анализ угроз безопасности информационной системы?
- Что включает в себя разработка системы защиты информации?
- Как проверяется эффективность защиты информации в информационной системе?

Приложение 1

Краткие сведения из теории

Инженерно-техническая защита информации (ИТЗИ) — это комплекс мер и средств, направленных на обеспечение защиты информации в информационной системе (ИС) от утечки, разглашения, порчи, несанкционированного доступа и других угроз. Она включает в себя следующие этапы:

1. Анализ угроз безопасности ИС;
2. Разработка системы защиты информации;
3. Реализация системы защиты информации;
4. Проверка эффективности защиты информации;
5. Постоянный мониторинг и совершенствование системы защиты информации.

Лабораторная работа 7.
ВЫЯВЛЕНИЕ И ФИКСАЦИЯ СЛЕДОВ ПРОТИВОПРАВНОЙ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ДЕЯТЕЛЬНОСТИ

1. Цель работы: познакомиться с методами выявления и фиксации следов противоправной деятельности, связанной с использованием компьютерной деятельности, а также с возможными методами защиты от таких действий.

2. Задачи работы:

- рассмотреть типичные примеры противоправной деятельности, связанной с компьютерной деятельностью;
- изучить методы выявления и фиксации следов противоправной деятельности;
- рассмотреть методы защиты от противоправной деятельности, связанной с компьютерной деятельностью.

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;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- использовать средства физической защиты линий связи ИТКС;

Знать:

- 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 3.2Проводить 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 и порядок выполнения работы

1. Выберите известный киберпреступников (например, Кевин Митник) и проведите исследование его противоправных действий, связанных с компьютерной деятельностью. Составьте отчет, в котором перечислите действия, нарушенные законы и способы их выявления и предотвращения.
2. Напишите инструкцию для пользователя, как защитить свой компьютер от хакерских атак.

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

- Что такое противоправная деятельность, связанная с компьютерной деятельностью?
- Какие методы выявления следов противоправной деятельности существуют?
- Какие методы защиты от противоправной деятельности, связанной с компьютерной деятельностью, существуют?
- Какую роль играют брандмауэры в защите от противоправной деятельности?
- Что такое антивирусное программное обеспечение и как оно работает?

Приложение 1

Краткие сведения из теории

Противоправная деятельность, связанная с компьютерной деятельностью, может включать в себя взломы, кражи личных данных, вирусы и мошенничество. Выявление и фиксация следов такой деятельности может включать в себя мониторинг сетевой активности, анализ логов и системных журналов, а также использование специализированного программного обеспечения. Для защиты от противоправной деятельности можно использовать антивирусное программное обеспечение, брандмауэры, средства шифрования и установку обновлений ПО.

Лабораторная работа 8.
ИССЛЕДОВАНИЕ УРОВНЯ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ПК

1. Цель работы: изучение уровня побочного электромагнитного излучения персональных компьютеров (ПК) и способов его уменьшения.

2. Задачи работы:

- Изучить принципы электромагнитного излучения ПК и его влияния на здоровье человека.
- Определить уровень побочного электромагнитного излучения ПК с помощью специализированного оборудования.
- Изучить методы уменьшения уровня побочного электромагнитного излучения ПК.
- Провести практическое занятие по уменьшению уровня побочного электромагнитного излучения ПК.

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;

Знать:

- 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 и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:

- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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.

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание

Измерить уровень побочного электромагнитного излучения ПК в различных режимах его работы (например, во время загрузки операционной системы, при запуске приложений, при работе с интернетом). Сделать выводы о наиболее эмитирующих компонентах ПК и предложить методы уменьшения уровня излучения.

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

- Что такое побочное электромагнитное излучение?
- Какие факторы влияют на уровень побочного электромагнитного излучения ПК?

Приложение 1

Краткие сведения из теории

Персональные компьютеры, как и любое электронное устройство, испускают электромагнитное излучение в окружающую среду. Это излучение может негативно влиять на здоровье человека, вызывая головные боли, утомляемость, нарушения сна и другие проблемы. Уровень побочного электромагнитного излучения ПК зависит от многих факторов, включая тип и качество комплектующих, качество заземления и экранирования, тип используемых кабелей и др. Для уменьшения уровня побочного электромагнитного излучения ПК можно использовать различные методы, такие как использование экранирующих устройств, установка фильтров на кабеля, правильная организация расположения рабочего места, использование мониторов с низкой эмиссией и др.

Лабораторная работа 9.
СНЯТИЕ ДИАГРАММЫ НАПРАВЛЕННОГО МИКРОФОНА

1. Цель работы: изучение принципов работы направленного микрофона и снятие диаграммы направленности.

2. Задачи работы:

- Изучить принципы работы направленного микрофона.
- Подготовить экспериментальное оборудование и установить направленный микрофон на специальной подставке.
- Снять диаграмму направленности микрофона при различных углах поворота и различных частотах звука.
- Обработать полученные данные и проанализировать полученную диаграмму направленности.

Студент должен:

Иметь практический опыт:

- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

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;

Знать:

- 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 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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.

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание

Снять диаграмму направленности микрофона при помощи звукового генератора и осциллографа. Необходимо подать на микрофон сигнал на разных частотах и углах поворота и затем проанализировать полученную диаграмму направленности.

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

- Что такое направленный микрофон и как он работает?
- Какие типы направленных микрофонов существуют?
- Что такое диаграмма направленности микрофона и для чего она используется?
- Как влияет частота звука на диаграмму направленности микрофона?

Приложение 1

Краткие сведения из теории

Направленный микрофон является устройством, способным улавливать звук из определенного направления. Он работает на основе интерференции звуковых волн, которые приходят к микрофону из разных направлений. Конструкция направленного микрофона позволяет создать зону чувствительности в определенном направлении и уменьшить зону чувствительности в других направлениях.

Лабораторная работа 10.
ИССЛЕДОВАНИЕ СПЕКТРА РЕЧЕВОГО СИГНАЛА

1. **Цель работы**: познакомиться с методами исследования спектра речевого сигнала и применением полученных знаний для решения задач в области обработки звука.

2. **Задачи работы:**
   - Изучить теоретические основы спектрального анализа звуковых сигналов.
   - Освоить методы снятия спектра речевого сигнала с помощью программного обеспечения для обработки аудио.
   - Определить основные параметры спектра речевого сигнала, такие как частота основной гармоники, частота формант, ширина полосы пропускания и т.д.
   - Применить полученные знания для решения задач по анализу и обработке речевых сигналов.

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 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;

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**

снять спектр речевого сигнала с помощью программного обеспечения для обработки аудио (например, Audacity), определить частоту основной гармоники и частоты формант, построить график спектра.

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 спектр звукового сигнала?
2) Что такое спектральный анализ звукового сигнала?
3) Какие параметры спектра речевого сигнала можно определить?
4) Для чего используются результаты спектрального анализа речевого сигнала?

Приложение 1

Краткие сведения из теории

Спектр звукового сигнала - это графическое представление зависимости амплитуды звуковых колебаний от частоты. Спектральный анализ звукового сигнала позволяет определить частотные характеристики сигнала, такие как частоту основной гармоники, частоту формант, ширину полосы пропускания и т.д.

Лабораторная работа 11.
ОПРЕДЕЛЕНИЕ УРОВНЯ ПОБОЧНОГО ИЗЛУЧЕНИЯ В КАНАЛЕ ЭЛЕКТРОСВЯЗИ

1. **Цель работы**: познакомиться с методами определения уровня побочного излучения в канале электросвязи.
2. **Задачи работы:**
   - изучить теоретические основы побочного излучения в канале электросвязи;
   - ознакомиться с методами измерения уровня побочного излучения;
   - провести измерения уровня побочного излучения с помощью приборов;
   - проанализировать результаты измерений и сделать выводы.

Студент должен:
Иметь практический опыт:

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

Уметь:

- 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;

Знать:

- 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 3.2Проводить 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 и порядок выполнения работы**

1. Подготовить приборы для измерения побочного излучения.
2. Установить приборы на расстоянии 1 метр от кабеля электросвязи.
3. Измерить уровень побочного излучения в разных точках кабеля.
4. Составить отчет о результатах измерений.

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 побочное излучение в канале электросвязи?
2. Какие приборы используются для измерения уровня побочного излучения?

3. Какие факторы влияют на уровень побочного излучения в канале электросвязи?
4. Какие последствия может вызвать побочное излучение для электронных устройств?

Приложение 1

Краткие сведения из теории

Побочное излучение в канале электросвязи – это излучение электромагнитных волн, возникающих в процессе передачи сигнала по кабелю. Оно может влиять на другие кабели и электронные устройства, вызывая помехи и сбои в их работе. Для измерения уровня побочного излучения используются специальные приборы, такие как магнитные поляризаторы и датчики поля. Они позволяют измерять уровень излучения в разных точках кабеля и определять его воздействие на окружающие объекты.

Лабораторная работа 12.
ОПРЕДЕЛЕНИЕ УРОВНЯ ПОБОЧНОГО ИЗЛУЧЕНИЯ В КАНАЛЕ ВИБРОАКУСТИКИ

1. **Цель работы**: изучение методов определения уровня побочного излучения в канале виброакустики и оценка его воздействия на окружающую среду.
2. **Задачи работы:**
   - изучение теоретических основ побочного излучения в канале виброакустики;
   - ознакомление с методами измерения уровня побочного излучения;
   - определение уровня побочного излучения в канале виброакустики на практике;
   - оценка воздействия побочного излучения на окружающую среду и здоровье людей.

Студент должен:
Иметь практический опыт:

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

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;

Знать:

- 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 3.2Проводить 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. Собрать установку для исследования уровня побочного излучения в канале виброакустики.
2. Провести измерения побочного излучения в канале виброакустики при различных режимах работы установки.
3. Обработать полученные данные и определить уровень побочного излучения.
4. Сделать выводы на основе полученных результатов и сравнить их с теоретическими ожиданиями.

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 виброакустика?
2) Что такое канал виброакустики?
3) Что такое побочное излучение в канале виброакустики?

Приложение 1

Краткие сведения из теории

Виброакустика – это наука, изучающая звуковые колебания твердых тел, вызванные механическими воздействиями на эти тела. Канал виброакустики – это канал передачи звука через твердое тело, например, через стену или металлическую конструкцию. При передаче звука через такие твердые тела происходит побочное излучение – излучение звуковых волн из тела, которое не является источником звука. Уровень побочного излучения в канале виброакустики зависит от различных факторов, таких как материалы, из которых состоит твердое тело, его размеры, частота звука и т.д.

Побочное излучение в канале виброакустики представляет собой энергию, которая не попадает в зону, предназначенную для ее передачи, а распространяется в сторону окружающей среды. Уровень побочного излучения зависит от многих факторов, таких как конструкция виброакустической системы, материалы, используемые при изготовлении, частотный диапазон, настройка и другие.

Одним из методов измерения уровня побочного излучения является использование спектроанализатора. Он позволяет измерять амплитуду и частоту побочного излучения и оценить его воздействие на окружающую среду.

Лабораторная работа 13.
ИЗМЕРЕНИЕ УРОВНЯ МАСКИРУЮЩЕГО ВИБРОАКУСТИЧЕСКОГО ШУМА

1. **Цель работы**: ознакомиться с методами измерения уровня маскирующего виброакустического шума и определения его влияния на качество звука.

2. **Задачи работы:**
   - Изучить теоретические основы маскировки звука и методы измерения уровня маскирующего виброакустического шума.
   - Ознакомиться с приборами и оборудованием, необходимым для проведения измерений.
   - Провести измерения уровня маскирующего виброакустического шума в различных условиях.
   - Обработать полученные данные и сделать выводы о влиянии уровня маскирующего шума на качество звука.

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 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:
- 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;

ПК:
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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 измерение уровня маскирующего виброакустического шума в комнате с различной степенью звукоизоляции. Сравнить результаты измерений и сделать выводы о влиянии степени звукоизоляции на уровень маскирующего шума.

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 маскировка звука?
2) Какими единицами измеряется уровень маскирующего виброакустического шума?
3) Как проводится измерение уровня маскирующего виброакустического шума?
4) Каковы факторы, влияющие на уровень маскирующего виброакустического шума?

Приложение 1

Краткие сведения из теории

Маскировка звука - это явление, когда наличие шума или другого звука скрывает или затрудняет восприятие другого звука. Виброакустический шум - это нежелательный звук, возникающий в результате вибрации различных поверхностей в окружающей среде. Уровень маскирующего виброакустического шума измеряется в децибелах (дБ) и определяется как разность между уровнем маскирующего шума и уровнем исходного звука.

Лабораторная работа 14.
ИЗМЕРЕНИЕ УРОВНЯ МАСКИРУЮЩЕГО ЦИФРОВОГО ШУМА

1. **Цель работы**: ознакомление с методами измерения уровня маскирующего цифрового шума и применение полученных знаний на практике.
2. **Задачи работы:**
   - изучение основных понятий и теоретических сведений о маскирующем цифровом шуме;
   - изучение методов измерения уровня маскирующего цифрового шума;
   - практическое применение методов измерения уровня маскирующего цифрового шума на конкретном оборудовании.

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 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:

- 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;
- 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**

измерение уровня маскирующего цифрового шума с помощью спектроанализатора на конкретном оборудовании.

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 маскирующий цифровой шум?
2) Какие методы измерения уровня маскирующего цифрового шума существуют?
3) Как спектроанализатор помогает в измерении уровня маскирующего цифрового шума?
4) Каким образом маскирующий цифровой шум может повлиять на качество звука?

Приложение 1

Краткие сведения из теории

Маскирующий цифровой шум — это шум, который возникает в процессе цифровой обработки сигнала и может привести к снижению качества воспроизведения звука. Методы измерения уровня маскирующего цифрового шума включают использование спектроанализаторов, которые могут показать частотную составляющую шума.

Лабораторная работа 15.
ИСПЫТАНИЕ УЧЕБНОЙ АУДИТОРИИ НА УТЕЧКУ ИНФОРМАЦИИ ПО КАНАЛУ ПЭМИН

1. Цель работы: изучение методов и инструментов для обнаружения и предотвращения утечки информации по каналу ПЭМИН

2. Задачи работы:

- Изучение теоретических основ утечки информации по каналу ПЭМИН.
- Ознакомление с инструментами и методами обнаружения утечки информации.
- Испытание учебной аудитории на утечку информации по каналу ПЭМИН.
- Оценка результатов и подготовка отчета.

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 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:

- 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;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- 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

1. Подготовьте два компьютера и соедините их с помощью сетевого кабеля.
2. Запустите на одном компьютере программу, которая будет отправлять информацию по сетевому кабелю.
3. Используя инструменты для обнаружения утечки информации (например, анализатор спектра), определите, возможно ли перехватывать передаваемую информацию по каналу ПЭМИН.

4. Если утечка информации обнаружена, примените меры по ее предотвращению.

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 информации по каналу ПЭМИН?
2) Какие методы используются для обнаружения утечки информации по каналу ПЭМИН?
3) Какие меры можно принять для предотвращения утечки информации по каналу ПЭМИН?

Приложение 1

Краткие сведения из теории

Утечка информации по каналу ПЭМИН возникает, когда проводной кабель или другое устройство излучает электромагнитные волны, содержащие информацию, которая может быть перехвачена по воздуху или другому проводнику. Это может произойти из-за необходимости передачи большого объема данных или из-за ошибок проектирования или эксплуатации оборудования. Обнаружение утечки информации по каналу ПЭМИН может быть осуществлено с помощью различных методов, включая анализ спектра излучения, поиск и анализ магнитных полей, анализ временных диаграмм сигналов и других техник.

Лабораторная работа 16.
ИСПЫТАНИЕ УЧЕБНОЙ АУДИТОРИИ НА УТЕЧКУ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

1. **Цель работы**: изучение вопросов безопасности информации и определение возможности утечки конфиденциальной информации из учебной аудитории по виброакустическому каналу.
2. **Задачи работы:**
   - Определить возможность утечки информации из учебной аудитории по виброакустическому каналу.
   - Определить уровень шума в аудитории, который может влиять на возможность утечки информации.
   - Изучить методы защиты от утечки информации по виброакустическому каналу.
   - Предложить рекомендации по защите от утечки информации в учебной аудитории.

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 техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- 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;
- 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**

Изучение уровня шума и возможности утечки информации по виброакустическому каналу в учебной аудитории. Для этого необходимо провести звуковое измерение уровня шума в аудитории при различных условиях (например, при различных количествах студентов в аудитории) и провести эксперимент по передаче информации через виброакустический канал.

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) Каким образом виброакустический канал может быть использован для утечки конфиденциальной информации?
3) Какими методами можно защититься от утечки информации по виброакустическому каналу?
4)

Приложение 1

Краткие сведения из теории

Виброакустический канал - это канал связи, основанный на преобразовании акустических вибраций, возникающих в твердых телах, в электрические сигналы. Вибрации в твердых телах могут передаваться на значительные расстояния и могут использоваться для передачи звуковой информации. Виброакустический канал может быть использован для утечки конфиденциальной информации из помещений, поэтому важно изучить возможности и методы защиты от такой утечки.