

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ

по дисциплине

«Защита информации от утечки по техническим каналам»

для студентов

Специальности 10.05.03 Информационная безопасность

автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Оглавление

Введение	4
Лабораторная работа 1 исследование акустических каналов утечки информации	5
Лабораторная работа 2 исследование электромагнитных излучений пэвм ..	7
Лабораторная работа 3 анализ наводок в цепях электропитания.....	10
Лабораторная работа 4 защита от утечки информации через линии связи.	13
Лабораторная работа 5 выявление закладных устройств с использованием нелинейных локаторов	16
Лабораторная работа 6 исследование оптических каналов утечки информации (лазерные микрофоны).....	18
Лабораторная работа 7 анализ побочных излучений от средств мобильной связи	21
Лабораторная работа 8 защита информации в беспроводных сетях (wi-fi, bluetooth).....	24
Лабораторная работа 9 исследование акустических свойств строительных конструкций	28
Лабораторная работа 10 методы подавления диктофонов и аудиозаписывающих устройств	31
Лабораторная работа 11 защита от утечки информации через тепловые каналы	34
Список литературы.....	39

Введение

Защита информации от утечки по техническим каналам представляет собой комплекс организационных и технических мероприятий, направленных на предотвращение несанкционированного получения информации через побочные излучения и наводки технических средств. Основным признаком технического канала утечки является возможность дистанционного перехвата информации без физического доступа к защищаемому объекту.

Проблема защиты информации от утечки по техническим каналам возникла в середине XX века с появлением электронных средств обработки информации. Исторически первые исследования в этой области связаны с работами по электромагнитной совместимости и защите от радиоперехвата, которые проводились в 1950-1960 годах. Значительный вклад в развитие теории технической защиты информации внесли исследования в рамках программы TEMPEST, инициированной правительством США.

Современные технические каналы утечки информации можно классифицировать по следующим видам:

- Электромагнитные (побочные излучения аппаратуры)
- Акустические (вибрационные колебания конструкций)
- Оптические (лазерные и тепловые методы съема)
- Параметрические (изменение параметров окружающей среды)

Курс лабораторных работ состоит из одиннадцати лабораторных работ, списка литературы и оглавления. Предлагаемое учебное пособие предназначено для студентов, обучающихся по специальности: 10.05.03 «Информационная безопасность автоматизированных систем».

Лабораторная работа 1 исследование акустических каналов утечки информации

Цель и содержание: изучение принципов формирования акустических каналов утечки информации, освоение методов измерения параметров акустических сигналов, оценка эффективности звукоизоляционных материалов.

Теоретическое обоснование

Акустический канал утечки информации представляет собой физический путь распространения звуковых волн, по которому возможна несанкционированная передача речевой или технической информации. В практике защиты информации различают три основных типа акустических каналов утечки.

Первый тип - прямая акустическая утечка, при которой звуковые волны распространяются непосредственно в воздушной среде. Этот канал характерен для передачи речевой информации в помещениях и шумов работающего оборудования. Основными параметрами, характеризующими данный канал, являются уровень звукового давления, частотный спектр и направленность излучения.

Второй тип - виброакустический канал, где передача информации происходит через колебания твердых конструкций здания: стен, перекрытий, оконных стекол, вентиляционных каналов и трубопроводов. Особую опасность представляют стеклянные поверхности, обладающие высокой звукопроводимостью. Эффективность передачи колебаний зависит от физических свойств материалов, их толщины и конструктивных особенностей.

Третий тип - параметрический канал, возникающий при модуляции электромагнитных полей акустическими колебаниями. Такое явление наблюдается в силовых кабелях, линиях связи и электронных устройствах. Для выявления подобных каналов требуется специальное измерительное оборудование.

Нормативные требования к защите от акустической утечки информации регламентируются ГОСТ Р 50922-2006 и СНиП 23-03-2003. Согласно этим документам, предельно допустимый уровень звукового давления в помещениях для конфиденциальных переговоров не должен превышать 35 дБА для речевой информации и 25 дБА для технических каналов. Требования к звукоизоляции ограждающих конструкций устанавливают минимальный индекс звукоизоляции 45 дБ для стен и 35 дБ для оконных конструкций.

Аппаратура и материалы

Для проведения исследований используется следующий комплект оборудования:

1. Измерительный комплекс, включающий шумомер "Октава-110А" первого класса точности с диапазоном измерений 30-130 дБ, анализатор спектра "СК4-72" с полосой пропускания 20 Гц - 50 кГц и генератор сигналов ГЗ-112/1 с точностью

0,5%.

2. Виброметрическое оборудование: вибродатчик ДВ-3 с усилителем УВ-2, лазерный виброметр "ЛВ-01" с диапазоном измерений 0,1-10000 Гц и четырехканальный осциллограф С1-94.

3. Дополнительное оборудование: направленный микрофон МКЭ-378 с чувствительностью 5 мВ/Па, набор звукопоглощающих материалов толщиной 30-100 мм и эталонный источник звука "ЭИЗ-1".

Методика и порядок выполнения работы

Исследование акустических каналов утечки информации включает несколько этапов. Первый этап - измерение фонового шума в помещении. Шумомер устанавливается на штативе на высоте 1,5 метра от пола, включается режим "Lin" с временной характеристикой "Fast". После калибровки с использованием эталонного источника проводятся измерения в пяти контрольных точках помещения при различных режимах работы оборудования. Результаты обрабатываются по формуле эквивалентного уровня звука и представляются в виде карты распределения шума.

Второй этап - оценка звукоизоляции строительных конструкций. Источник звука устанавливается на расстоянии 1 метра от исследуемой конструкции, в приемном помещении размещается измерительный микрофон. Измерения проводятся на шести стандартных частотах, после чего рассчитывается индекс звукоизоляции и строится частотная характеристика.

Третий этап включает анализ полученных данных, выявление потенциальных каналов утечки и оценку эффективности звукоизоляционных материалов. По результатам измерений составляются рекомендации по улучшению акустической защиты помещения.

Содержание отчета

Отчет должен содержать:

1. Титульный лист с указанием названия дисциплины, темы работы, фамилии студента и преподавателя.
2. Основную часть с протоколами измерений, результатами расчетов и графиками.
3. Выводы с оценкой акустической безопасности помещения и рекомендациями по защите.

Вопросы для защиты работы

1. Какие существуют типы акустических каналов утечки информации?
2. Какими параметрами характеризуется акустический сигнал?
3. Какие нормативные документы регламентируют защиту от акустической утечки?
4. Какое оборудование используется для исследования акустических каналов?
5. Как оценивается эффективность звукоизоляционных материалов?

Лабораторная работа 2 исследование электромагнитных излучений пэвм

Цель работы:

Измерить уровни побочных электромагнитных излучений (ПЭМИ) и наводок (ПЭМН) от системного блока, монитора и периферийных устройств.

Оценить эффективность экранирования корпусов и кабелей.

Оборудование и материалы

Персональный компьютер (системный блок, ЖК/ЭЛТ-монитор).

Периферийные устройства (клавиатура, мышь, принтер).

Спектроанализатор (или осциллограф с широкополосным датчиком).

Антенна ближнего поля (петлевая или рамковая).

Индуктивный датчик для измерения наводок в кабелях.

Экранирующие материалы (алюминиевая фольга, медная сетка).

Измеритель напряженности электромагнитного поля.

Ход работы

1. Подготовка к измерениям

Организация рабочего места:

Установите ПК и монитор на деревянный или пластиковый стол (металлические поверхности могут исказить измерения).

Расположите измерительную аппаратуру на расстоянии 0.5–1 м от исследуемых устройств.

Убедитесь, что в помещении отсутствуют посторонние источники помех (Wi-Fi-роутеры, мобильные телефоны, другие ПК).

Настройка измерительных приборов:

Включите спектроанализатор и установите диапазон частот:

Низкие частоты (0–100 кГц) – для наводок в цепях питания.

Средние частоты (100 кГц – 100 МГц) – для излучений от шин данных.

Высокие частоты (100 МГц – 3 ГГц) – для процессора, видеокарты, беспроводных модулей.

Подключите антенну ближнего поля к спектроанализатору.

2. Измерение ПЭМИН без экранирования

2.1. Системный блок

Включите ПК и запустите программу, создающую высокую нагрузку на процессор (например, стресс-тест AIDA64).

Измерьте излучения:

Вблизи процессора – установите антенну над вентиляционными отверстиями.

Вблизи видеокарты – измерьте излучения в области PCI-E слота.

Вблизи блока питания – зафиксируйте помехи на частотах 50–100 кГц (импульсные преобразователи).

Запишите максимальные уровни сигналов в таблицу:

Компонент ПК	Частота, МГц	Уровень излучения, дБмкВ
--------------	--------------	--------------------------

Процессор	2400	45
-----------	------	----

Видеокарта	1500	52
------------	------	----

Блок питания	0.1	38
--------------	-----	----

2.2. Монитор

Включите монитор и установите режим максимального разрешения.

Измерьте излучения:

Вблизи экрана – для ЖК-мониторов (частота ШИМ подсветки, ~200 Гц).

Вблизи схемы управления – для ЭЛТ (частота строчной развертки, 15–100 кГц).

Запишите данные.

2.3. Периферийные устройства

Подключите USB-устройства (флешку, мышь).

Измерьте наводки в кабелях с помощью индуктивного датчика.

Зафиксируйте уровень помех при передаче данных.

3. Оценка эффективности экранирования

3.1. Экранирование системного блока

Оберните корпус системного блока алюминиевой фольгой (с заземлением).

Повторите измерения в тех же точках.

Сравните результаты:

Компонент ПК	Без экрана, дБмкВ	С экраном, дБмкВ	Эффективность, дБ
Процессор	45	30	15

3.2. Экранирование кабелей

Замените неэкранированный USB-кабель на экранированный.

Измерьте уровень наводок.

Сравните результаты.

4. Анализ результатов

Постройте графики спектров излучения:

До и после экранирования.

Для разных компонентов ПК.

Сделайте выводы:

Какие узлы ПК создают наибольшие помехи?

Насколько эффективно экранирование?

Требования к отчету

Титульный лист

Теоретическая часть

Таблицы и графики измерений.

Расчет эффективности экранирования.

Выводы (анализ данных, рекомендации).

Вопросы для защиты

1. Почему процессор и видеокарта – основные источники ПЭМИН?
2. Как экранирование влияет на уровень излучений?
3. Какие методы защиты наиболее эффективны для кабелей?

Лабораторная работа 3 анализ наводок в цепях электропитания

Цель работы:

Обнаружение информационных сигналов в сетях электропитания 220 В.

Исследование эффективности фильтрующих устройств и развязывающих трансформаторов для подавления наводок.

Теоретическое обоснование

1. Наводки в цепях электропитания

При работе электронной аппаратуры в сети 220 В могут возникать паразитные сигналы, вызванные:

Импульсными источниками питания (компьютеры, мониторы, ИБП).

Коммутационными процессами (включение/выключение мощных нагрузок).

Электромагнитными наводками от соседних кабелей.

Эти наводки могут содержать **информационные составляющие**, что представляет угрозу утечки данных по техническим каналам.

2. Методы обнаружения наводок

Для анализа используются:

Осциллограф – визуализация формы напряжения и помех.

Спектроанализатор – определение частотного состава наводок.

Индуктивные датчики – съем сигналов с кабелей без гальванического контакта.

3. Методы защиты от наводок

Фильтрующие устройства (сетевые фильтры):

Подавляют высокочастотные помехи (выше 150 кГц).

Состоят из LC-цепей (дрессели, конденсаторы).

Развязывающие трансформаторы:

Гальваническая развязка сети и нагрузки.

Подавление синфазных помех.

Экранирование кабелей – уменьшение влияния внешних полей.

Оборудование и материалы

Осциллограф (полоса пропускания ≥ 100 МГц).

Спектроанализатор (диапазон 9 кГц – 3 ГГц).

Индуктивный датчик (токовые клещи).

Сетевой фильтр (с LC-цепями).

Развязывающий трансформатор (220 В / 220 В).

Нагрузка (ПК, импульсный блок питания).

3. Ход работы

1. Подготовка к измерениям

Схема подключения:

Подключите исследуемую нагрузку (ПК) к сети 220 В через развязывающий трансформатор или фильтр.

Установите осциллограф и спектроанализатор параллельно нагрузке.

Настройка приборов:

Осциллограф: режим АС-связи, полоса 20 МГц.

Спектроанализатор: диапазон 0–30 МГц.

2. Обнаружение наводок в сети 220 В

2.1. Измерение без фильтрации

Включите ПК и запустите стресс-тест (нагрузка на процессор).

Зафиксируйте осциллограмму напряжения в сети:

Низкочастотные помехи (50–150 Гц) – от работы импульсного БП.

Высокочастотные помехи (150 кГц – 30 МГц) – от ШИМ-контроллеров.

Запишите амплитуду и частоту наиболее значимых помех.

2.2. Анализ спектра помех

Подключите спектроанализатор через индуктивный датчик.

Зафиксируйте спектр помех:

Гармоники 50 Гц (100 Гц, 150 Гц).

Импульсные помехи (частота преобразования БП, 20–100 кГц).

Сравните спектры при разных режимах работы ПК (холостой ход, нагрузка).

3. Исследование фильтрующих устройств

3.1. Подключение сетевого фильтра

Установите фильтр между сетью и нагрузкой.

Повторите измерения осциллографом и спектроанализатором.

Оцените подавление помех:

Высокочастотные составляющие должны уменьшиться на 20–40 дБ.

3.2. Использование развязывающего трансформатора

Подключите нагрузку через трансформатор.

Зафиксируйте изменения:

Исчезновение синфазных помех.

Снижение уровня гармоник.

Сравните результаты с фильтром.

4. Оформление результатов

Постройте графики:

Осциллограммы напряжения до и после фильтрации.

Спектры помех при разных методах защиты.

Рассчитайте эффективность фильтрации:

$$K = 20 \cdot \log_{10} \left(\frac{U_1}{U_2} \right), \text{дБ} \quad K = 20 \cdot \log_{10} \left(\frac{U_2}{U_1} \right), \text{дБ}$$

где U_1 – уровень помех без фильтра, U_2 – с фильтром.

Требования к отчету

Титульный лист

Теоретическая часть

Результаты измерений (таблицы, осциллограммы, спектры).

Выводы (эффективность фильтров и трансформаторов).

Вопросы для защиты

1. Какие виды помех встречаются в сети 220 В?
2. Как отличить информационную наводку от фоновой помехи?
3. Почему развязывающий трансформатор эффективнее фильтра?
4. Какие параметры фильтра влияют на подавление помех?

Лабораторная работа 4 защита от утечки информации через линии связи

Цель работы:

Измерение паразитной модуляции в телефонных и Ethernet-кабелях.

Тестирование эффективности защитных устройств (линейные развязки, фильтры).

Теоретическое обоснование

1. Каналы утечки информации через линии связи

При передаче данных по кабелям возможно возникновение побочных излучений и наводок, которые могут привести к перехвату информации. Основные каналы утечки:

Гальваническая связь – через общие цепи питания и заземления.

Индуктивная и емкостная связь – за счет электромагнитного влияния между проводами.

Паразитная модуляция – наложение информационных сигналов на несущие частоты.

2. Методы измерения паразитной модуляции

Для анализа используются:

Высокочастотный осциллограф – для визуализации сигналов.

Спектроанализатор – для определения частотных характеристик наводок.

Индуктивные и емкостные датчики – для съема сигналов без прямого контакта.

3. Защитные устройства

Линейные развязки (оптроны, трансформаторы) – обеспечивают гальваническую развязку.

Фильтры высоких и низких частот – подавляют паразитные сигналы.

Экранированные кабели – уменьшают влияние внешних электромагнитных полей.

Оборудование и материалы

Телефонная линия и Ethernet-кабель.

Осциллограф (полоса пропускания ≥ 100 МГц).

Спектроанализатор (диапазон 9 кГц – 3 ГГц).

Индуктивные и емкостные датчики.

Линейные развязки (оптронные или трансформаторные).

Фильтры ВЧ и НЧ.

Экранированные кабели.

Ход работы

1. Подготовка к измерениям

Схема подключения:

Подключите телефонный аппарат и компьютер к соответствующим линиям.

Установите осциллограф и спектроанализатор параллельно линиям связи.

Настройка приборов:

Осциллограф: режим АС-связи, полоса 20 МГц.

Спектроанализатор: диапазон 0–30 МГц.

2. Измерение паразитной модуляции

2.1. Телефонная линия

Включите телефон и создайте тестовый сигнал (тональный набор или голосовое сообщение).

Зафиксируйте осциллограмму напряжения в линии:

Низкочастотные сигналы (300 Гц – 3.4 кГц) – полезный сигнал.

Высокочастотные наводки (выше 4 кГц) – паразитная модуляция.

Запишите амплитуду и частоту паразитных сигналов.

2.2. Ethernet-кабель

Подключите компьютер к сети и запустите передачу данных.

Зафиксируйте осциллограмму напряжения в кабеле:

Основные гармоники (1–100 МГц) – полезный сигнал.

Паразитные составляющие (выше 100 МГц) – наводки.

Сравните спектры при разных режимах передачи (холостой ход, нагрузка).

3. Тестирование защитных устройств

3.1. Линейные развязки

Установите оптронную или трансформаторную развязку в телефонную линию.

Повторите измерения осциллографом и спектроанализатором.

Оцените подавление паразитных сигналов:

Гальваническая развязка должна устранить низкочастотные наводки.

3.2. Фильтры ВЧ и НЧ

Подключите фильтр к Ethernet-кабелю.

Зафиксируйте изменения:

Фильтр НЧ подавляет высокочастотные помехи.

Фильтр ВЧ устраняет низкочастотные наводки.

Сравните результаты с развязками.

3.3. Экранированные кабели

Замените обычный кабель на экранированный.

Измерьте уровень наводок.

Сравните результаты с предыдущими методами.

4. Оформление результатов

Постройте графики:

Осциллограммы сигналов до и после защиты.

Спектры паразитных составляющих.

Рассчитайте эффективность защитных устройств:

$$K = 20 \cdot \log_{10} \left(\frac{U_1}{U_2} \right), \text{дБ} \quad K = 20 \cdot \log \left(\frac{U_2}{U_1} \right), \text{дБ}$$

где U_1 – уровень помех без защиты, U_2 – с защитой.

Требования к отчету

Титульный лист

Теоретическая часть

Результаты измерений (таблицы, осциллограммы, спектры).

Выводы (эффективность защитных устройств).

Вопросы для защиты

1. Какие виды паразитной модуляции встречаются в линиях связи?
2. Как линейные развязки защищают от утечки информации?
3. Какие параметры фильтров влияют на подавление помех?
4. Почему экранированные кабели эффективнее обычных?

Лабораторная работа 5 выявление закладных устройств с использованием нелинейных локаторов

Цель работы:

Изучение принципов работы нелинейных радиолокаторов.

Практический поиск скрытых электронных устройств (радиомикрофонов, жучков) в помещении.

Теоретическое обоснование

1. Нелинейная локация: физические основы

Нелинейные локаторы (НЛ) обнаруживают электронные устройства по их способности к нелинейному преобразованию радиосигналов. Принцип действия основан на:

Генерации гармоник – полупроводниковые элементы (диоды, транзисторы) в электронных схемах преобразуют зондирующий сигнал, создавая гармоники ($2f$, $3f$ и т.д.).

Переизлучении комбинационных частот – при воздействии двух сигналов (f_1 и f_2) закладные устройства генерируют частоты $f_1 \pm f_2$.

2. Типы закладных устройств

Активные (радиопередатчики, GSM-жучки) – излучают сигнал самостоятельно.

Пассивные (акустические резонаторы, нелинейные отражатели) – требуют внешнего облучения для детектирования.

3. Методы защиты помещений

Регулярные проверки НЛ и спектроанализаторами.

Экранирование стен и окон (металлические сетки, фольгированные материалы).

Использование подавителей связи (глушилок) в охраняемых зонах.

Оборудование и материалы

Нелинейный локатор (например, "Пиранья" или АНЛ-2).

Тестовые закладные устройства (радиомикрофон, жучок с диодным детектором).

Спектроанализатор (диапазон 1 МГц – 6 ГГц).

Ноутбук с ПО для обработки сигналов (по необходимости).

Экранирующие материалы (металлизированная ткань, фольга).

Ход работы

1. Подготовка оборудования

Настройка локатора:

Установите частоту зондирующего сигнала (обычно 900 МГц – 2.5 ГГц).

Включите режим детектирования 2-й и 3-й гармоник.

Калибровка:

Проверьте работу НЛ на тестовом объекте (диод, транзистор).

Зафиксируйте уровень фоновых сигналов в помещении.

2. Поиск закладных устройств

2.1. Обследование помещения

Методика сканирования:

Перемещайте антенну локатора вдоль стен, мебели, розеток (скорость ≤ 0.5 м/с).

Особое внимание уделите:

Вентиляционным решеткам.

Электроприборам (лампы, блоки питания).

Потолочным конструкциям.

Фиксация сигналов:

При обнаружении гармоник (2f, 3f) определите местоположение источника.

Используйте спектроанализатор для уточнения частотных характеристик.

2.2. Тестирование экранирования

Накройте подозрительный объект экранирующим материалом.

Повторите измерения:

Эффективное экранирование снижает уровень гармоник на ≥ 20 дБ.

3. Анализ результатов

Постройте карту помещения с отметками обнаруженных аномалий.

Определите тип устройства по спектральным характеристикам:

Диодные детекторы – четкие 2-я и 3-я гармоники.

Транзисторные схемы – широкий спектр комбинационных частот.

Рассчитайте дальность обнаружения для разных типов закладок.

Требования к отчету

Титульный лист

Теоретическая часть (принципы НЛ, виды закладок).

Результаты обследования (карта помещения, спектрограммы).

Выводы (эффективность методов, рекомендации по защите).

Вопросы для защиты

1. Чем отличается нелинейная локация от традиционной радиолокации?
2. Почему диоды и транзисторы хорошо обнаруживаются НЛ?
3. Как экранирование влияет на работу закладных устройств?
4. Какие частоты наиболее эффективны для зондирования?

Лабораторная работа 6 исследование оптических каналов утечки информации (лазерные микрофоны)

Цель работы:

Демонстрация принципа съёма акустической информации через вибрацию оконных стёкол с использованием лазерного микрофона.

Исследование методов противодействия оптическому каналу утечки информации.

Теоретическое обоснование

1. Принцип работы лазерного микрофона

Лазерный микрофон – устройство, позволяющее дистанционно регистрировать акустические колебания, преобразуя их в оптический сигнал. Принцип действия основан на:

Отражении лазерного луча от вибрирующей поверхности (стекло, зеркало, стена).

Доплеровском эффекте – изменении частоты отражённого луча при колебаниях поверхности.

Демодуляции сигнала – преобразовании оптических изменений в электрический сигнал.

2. Основные компоненты системы

Лазерный излучатель (обычно ИК-диапазона).

Приёмник отражённого сигнала (фотодиод с усилителем).

Система обработки сигнала (фильтры, демодуляторы).

3. Методы противодействия

Акустические помехи – генерация фонового шума для маскировки полезного сигнала.

Защитные плёнки – нанесение на стёкла покрытий, рассеивающих лазерный луч.

Вибрационные глушители – устройства, создающие контрвибрации стекла.

Затемнение окон – использование штор или жалюзи для блокировки лазерного луча.

Оборудование и материалы

Лазерный микрофон (например, базовый комплект на основе лазерного диода 650 нм).

Оконное стекло (размером не менее 50×50 см).

Акустический генератор сигналов (колонка или динамик).

Осциллограф (для визуализации сигнала).

Защитная плёнка для стёкол (с рассеивающим покрытием).

Источник акустических помех (белый шум).

Ход работы

1. Подготовка экспериментального стенда

Установите оконное стекло в раму, имитирующую оконный проём.

На расстоянии 5–10 м от стекла разместите лазерный микрофон, направленный на центр стекла.

Зафиксируйте лазерный луч на поверхности стекла.

Подключите выход фотоприёмника к осциллографу.

2. Демонстрация съёма информации

2.1. Регистрация акустических колебаний

Включите акустический генератор (например, воспроизведение речи с частотой

300–3400 Гц).

Зафиксируйте сигнал на осциллографе:

Без акустического воздействия – ровная линия (шум).

При воздействии звука – появление модулированного сигнала.

Определите порог чувствительности системы (минимальная громкость, при которой сигнал различим).

2.2. Анализ параметров сигнала

Измерьте амплитуду и частоту модуляции.

Сравните исходный акустический сигнал и сигнал, восстановленный с фотоприёмника.

3. Исследование методов противодействия

3.1. Акустические помехи

Включите генератор белого шума (50–60 дБ).

Повторите запись сигнала:

Без помех – чёткий речевой сигнал.

С помехами – сигнал маскируется шумом.

Оцените степень подавления полезного сигнала.

3.2. Защитные плёнки

Наклейте на стекло рассеивающую плёнку.

Повторите измерения:

Уровень отражённого сигнала должен снизиться на 20–30 дБ.

Сравните качество восстановления речи до и после нанесения плёнки.

3.3. Альтернативные методы (по возможности)

Вибрационные глушители – установите устройство, создающее случайные колебания стекла.

Затемнение окон – используйте шторы, оцените возможность фокусировки лазера.

4. Оформление результатов

Запишите осциллограммы:

Чистый сигнал.

Сигнал с помехами.

Сигнал после нанесения плёнки.

Постройте графики:

Зависимость уровня сигнала от расстояния до стекла.

Эффективность методов защиты (в % подавления).

Требования к отчету

Титульный лист

Теоретическая часть (принцип работы лазерного микрофона).

Результаты измерений (осциллограммы, графики).

Выводы (эффективность методов противодействия).

Вопросы для защиты

1. Как лазерный микрофон преобразует акустические колебания в электрический сигнал?
2. Какие параметры стекла влияют на качество съёма информации?
3. Почему защитные плёнки снижают эффективность лазерного микрофона?
4. Какие ещё методы защиты от оптических каналов утечки вы знаете?

Лабораторная работа 7 анализ побочных излучений от средств мобильной связи

Цель работы:

Обнаружение и анализ электромагнитных излучений, создаваемых смартфонами в различных режимах работы.

Оценка эффективности режима "полёт" и экранированных помещений для защиты от утечки информации.

Теоретическое обоснование

1. Побочные излучения смартфонов

Современные мобильные устройства являются источниками электромагнитных излучений в широком частотном диапазоне:

Основные рабочие частоты (GSM: 900/1800 МГц, 3G/4G: 1.9-2.7 ГГц, Wi-Fi:

2.4/5 ГГц)

Побочные излучения (гармоники рабочих частот, импульсные помехи от процессора)

Пассивное переизлучение (от металлических элементов корпуса)

2. Каналы утечки информации

Активные каналы (преднамеренные излучения):

Передача данных по сотовым сетям

Работа Wi-Fi/Bluetooth модулей

Побочные каналы (непреднамеренные излучения):

Излучения процессора и системной шины

Модуляция сигналов на элементах питания

3. Методы защиты

Режим "полёт" - программное отключение радиомодулей

Экранированные помещения (клетка Фарадея) - аппаратная изоляция устройства

Специальные чехлы с радиопоглощающими материалами

Оборудование и материалы

Смартфоны различных моделей (2-3 шт.)

Спектроанализатор (диапазон 100 МГц - 6 ГГц)

Антенна ближнего поля

Экранированная камера или экранирующий контейнер

Осциллограф с ВЧ-датчиком

Персональный компьютер для обработки данных

Ход работы

1. Подготовка измерительного комплекса

Настройте спектроанализатор:

Диапазон сканирования: 100 МГц - 3 ГГц

Полоса пропускания: 1 МГц

Время развёртки: 500 мс

Установите антенну ближнего поля на расстоянии 10 см от исследуемого смартфона

2. Измерение излучений в различных режимах

2.1. Активный режим (разговор, передача данных)

Включите голосовой вызов или передачу данных

Зафиксируйте:

Основные несущие частоты

Уровень сигнала (дБм)

Гармоники (2f, 3f)

Примерные данные для таблицы:

Режим работы	Основная частота	Уровень сигнала	Наличие гармоник
GSM-вызов	900 МГц	-45 дБм	Да (1800 МГц)
4G передача	2.6 ГГц	-50 дБм	Нет

2.2. Режим ожидания

Активируйте режим ожидания

Зафиксируйте периодические импульсы синхронизации с базовой станцией

2.3. Режим "полёт"

Включите авиарежим

Проверьте остаточные излучения:

Тактовые частоты процессора

Помехи от дисплея

3. Тестирование экранирования

3.1. Экранированный контейнер

Поместите активный смартфон в экранированную камеру

Измерьте уровень сигнала снаружи:

Эффективное экранирование должно давать ослабление ≥ 60 дБ

3.2. Сравнительный анализ

Сравните спектры:

На открытом пространстве

В экранированном помещении

В режиме "полёт"

4. Обработка результатов

Постройте сравнительные графики:

Уровень излучения в разных режимах

Эффективность экранирования

Рассчитайте коэффициент экранирования:

$$SE=20\cdot\log(E1E2),\text{дБ} \quad SE=20\cdot\log(E2E1),\text{дБ}$$

где $E1E1$ - поле без экранирования, $E2E2$ - с экранированием

Требования к отчету

Титульный лист

Теоретическая часть (кратко)

Результаты измерений (таблицы, графики спектров)

Выводы (оценка эффективности разных методов защиты)

Вопросы для защиты

1. Какие основные частоты излучают современные смартфоны?
2. Почему в режиме "полёт" остаются побочные излучения?
3. Как определить, что экранирование помещения эффективно?
4. Какие элементы смартфона создают наибольшие помехи?

Лабораторная работа 8 защита информации в беспроводных сетях (wi-fi, bluetooth)

Цель работы:

Исследование методов перехвата и анализа радиотрафика в беспроводных сетях.

Тестирование эффективности современных криптографических методов защиты (WPA3, VPN).

Теоретическое обоснование

1. Уязвимости беспроводных сетей

Беспроводные технологии Wi-Fi и Bluetooth подвержены ряду атак:
Пассивный перехват трафика (анализ незашифрованных данных).
Атаки "человек посередине" (MITM) – подмена точек доступа.
Деаутентификация – принудительное отключение устройств от сети.
Подбор паролей (атаки по словарю, перебор).

2. Методы защиты беспроводных сетей

2.1. Шифрование Wi-Fi

Протокол	Уровень защиты	Уязвимости
WEP	Низкий	Взлом за несколько минут
WPA	Средний	Уязвим к атакам типа KRACK
WPA2	Высокий	Уязвим к атакам на PMKID
WPA3	Максимальный	Устойчив к большинству атак

2.2. Дополнительные меры защиты

VPN (Virtual Private Network) – сквозное шифрование трафика.
MAC-фильтрация – ограничение доступа по физическим адресам.
Скрытие SSID – усложняет обнаружение сети.

Оборудование и материалы

Ноутбук с Wi-Fi-адаптером, поддерживающим режим мониторинга.

Смартфон с Bluetooth.

Программное обеспечение:

Aircrack-ng (анализ Wi-Fi).

Wireshark (перехват трафика).

Bluetooth Scanner (анализ Bluetooth-устройств).

Роутер с поддержкой WPA3.

VPN-сервис (например, OpenVPN или WireGuard).

Ход работы

1. Перехват и анализ Wi-Fi-трафика

1.1. Пассивный перехват

Переведите Wi-Fi-адаптер в режим мониторинга:

```
airmon-ng start wlan0
```

Запустите захват пакетов:

```
airodump-ng wlan0mon
```

Зафиксируйте:

SSID сетей.

Тип шифрования (WEP, WPA, WPA2, WPA3).

Уровень сигнала (RSSI).

1.2. Атака на WPA2 (имитация)

Запустите деаутентификацию клиента:

```
aireplay-ng --deauth 10 -a <BSSID> -c <ClientMAC> wlan0mon
```

Перехватите handshake-пакеты для последующего подбора пароля.

1.3. Анализ защищённых сетей (WPA3)

Попробуйте перехватить трафик WPA3-сети.

Убедитесь, что стандартные атаки (KRACK) не работают.

2. Анализ Bluetooth-трафика

2.1. Сканирование устройств

Запустите Bluetooth-сканер:

```
hcidtool scan
```

Определите:

MAC-адреса устройств.

Тип соединения (BLE/Classic).

2.2. Перехват данных (BLE Sniffing)

Используйте **Ubertooth** или **nRF Sniffer** для захвата пакетов.

Попробуйте декодировать незашифрованный трафик (например, данные с фитнес-браслета).

3. Тестирование методов защиты

3.1. Эффективность WPA3

Подключитесь к WPA3-сети.

Попробуйте перехватить трафик с помощью airodump-ng.

Сравните с WPA2 – убедитесь, что данные не расшифровываются.

3.2. Использование VPN

Подключитесь к открытой Wi-Fi-сети.

Запустите VPN и проверьте:

Можно ли перехватить реальный IP?

Виден ли трафик в Wireshark?

3.3. Дополнительные меры (MAC-фильтрация, скрытие SSID)

Включите фильтрацию по MAC-адресу на роутере.

Попробуйте подключиться с неразрешённого устройства.

Проверьте, помогает ли скрытие SSID против сканирования.

Оформление отчёта

1. Результаты измерений

Метод атаки	Тип защиты	Успешность перехвата
-------------	------------	----------------------

WPA2-PSK	WPA2	Успешно (handshake)
----------	------	---------------------

WPA3	SAE	Неуспешно
------	-----	-----------

Open Wi-Fi	VPN	Трафик зашифрован
------------	-----	-------------------

2. Выводы

WPA3 значительно надёжнее WPA2.

VPN полностью защищает трафик даже в открытых сетях.

MAC-фильтрация и скрытие SSID – слабая защита.

Вопросы для защиты

1. Чем WPA3 безопаснее WPA2?
2. Как VPN защищает данные в публичных Wi-Fi-сетях?
3. Почему Bluetooth-устройства уязвимы к перехвату?
4. Какие методы защиты Wi-Fi наиболее эффективны?

Лабораторная работа 9 исследование акустических свойств строительных конструкций

Цель работы:

Измерение индекса звукоизоляции стен, дверей и вентиляционных каналов.

Подбор оптимальных материалов для защиты от виброакустической утечки информации.

Теоретическое обоснование

1. Основные понятия звукоизоляции

Звукоизоляция – способность конструкции ослаблять проходящий через нее звук.

Оценивается:

Индексом звукоизоляции (R_w , дБ) – для воздушного шума

Уровнем виброизоляции – для ударного шума

2. Каналы утечки акустической информации

Прямое прохождение звука (через щели, тонкие перегородки)

Косвенная передача (через вибрации стен, инженерные коммуникации)

Резонансные явления (усиление звука на определенных частотах)

3. Нормативные требования

Конструкция	Минимальный R_w (дБ)
--------------------	--

Межкомнатные стены	43-52
--------------------	-------

Межквартирные стены	54-62
---------------------	-------

Двери в квартирах	32-37
-------------------	-------

Вентканалы	40-45
------------	-------

Оборудование и материалы

Измерительный комплекс:

Шумомер (класс 1, например, Октава-110А)

Генератор белого/розового шума

Частотный анализатор

Испытуемые конструкции:

Гипсокартонная перегородка

Деревянная дверь

Вентиляционный короб

Материалы для звукоизоляции:

Минеральная вата (плотность 30-50 кг/м³)

Звукоизоляционные мембраны (Тексаунд, Шуманет)

Демпферные ленты

Ход работы

1. Подготовка испытательного стенда

Соберите тестовые конструкции:

Перегородка 4×2.5 м (гипсокартон на металлокаркасе)

Дверной блок с коробкой

Вентиляционный канал длиной 2 м

Установите измерительные микрофоны:

С каждой стороны конструкции (источник/приемник)

На расстоянии 1 м от поверхности

2. Измерение звукоизоляции

2.1. Воздушный шум (R_w)

Подайте сигнал белого шума 100 дБ в "громкой" комнате

Зафиксируйте уровни в 1/3-октавных полосах:

Частота, Гц	Уровень в источнике, дБ	Уровень за перегородкой, дБ
-------------	-------------------------	-----------------------------

125	101	78
-----	-----	----

500	103	62
-----	-----	----

2000	102	45
------	-----	----

Рассчитайте R_w по формуле:

$$R_w = L_1 - L_2 + 10 \log \frac{S}{A} \quad R_w = L_1 - L_2 + 10 \log S/A$$

где S – площадь конструкции, A – эквивалентная площадь поглощения

2.2. Виброакустические измерения

Возбудите вибрации конструкции с помощью виброплатформы

Замерьте передачу вибраций:

На стыках конструкций

В точках крепления коммуникаций

3. Тестирование звукоизоляционных материалов

3.1. Многослойные конструкции

Последовательно добавляйте слои:

Гипсокартон 12 мм + минвата 50 мм

Двойной ГКЛ + Тексаунд 3 мм

Замерьте улучшение R_w для каждого варианта

3.2. Уплотнение притворов

Установите дверь с различными уплотнителями:

Поролоновая лента

Магнитный уплотнитель

Двойной контур

Измерьте разницу в звукоизоляции

Оформление результатов

1. Сводная таблица измерений

Конструкция	Исходный R_w	После модернизации	Прирост, дБ
Перегородка ГКЛ	42	56	+14
Деревянная дверь	28	38	+10
Вентканал	35	48	+13

2. Рекомендации по защите

Для стен:

Двойной каркас с перекрестным монтажом

Минвата + два слоя ГКЛ 12 мм

Для дверей:

Полотно не менее 40 кг

Тройной контур уплотнения

Для вентканалов:

Гибкие вставки

Шумоглушители

Вопросы для защиты

1. Чем отличается изоляция воздушного и ударного шума?
2. Почему низкие частоты (125 Гц) хуже изолируются?
3. Как влияет плотность материала на звукоизоляцию?
4. Какие ошибки монтажа снижают эффективность защиты?

Лабораторная работа 10 методы подавления диктофонов и аудиозаписывающих устройств

Цель работы:

Исследование методов генерации ультразвуковых и инфразвуковых помех для подавления работы диктофонов.

Тестирование эффективности детекторов диктофонов различных типов.

Теоретическое обоснование

1. Принципы работы диктофонов и их уязвимости

Современные диктофоны используют:

Чувствительные микрофоны (электретные, MEMS)

АЦП с полосой 20 Гц – 20 кГц

Фильтры шумоподавления

Уязвимости:

Чувствительность к ультразвуку (18–24 кГц) – вызывает перегрузку АЦП

Восприимчивость к инфразвуку (<20 Гц) – создает механические резонансы

Электромагнитные наводки – влияют на схемы обработки сигнала

2. Методы противодействия

2.1. Акустические помехи

Тип помех	Диапазон	Принцип воздействия
Ультразвуковые	18–24 кГц	Перегрузка входных цепей
Инфразвуковые	5–19 Гц	Вибрация корпуса
Широкополосные	0.1–25 кГц	Маскировка полезного сигнала

2.2. Детектирование диктофонов

RF-детекторы – обнаружение радиопередатчиков

Лазерные сканеры – выявление оптических элементов

Нелинейные локаторы – поиск полупроводниковых компонентов

Оборудование и материалы

Испытуемые устройства:

Аналоговый диктофон (Sony ICD-UХ570)

Цифровой диктофон с шумоподавлением

Смартфон в режиме записи

Генераторы помех:

Ультразвуковой (Velleman UMS20)

Инфразвуковой (спецгенератор 5–30 Гц)

Детекторы:

RF Explorer (для радиодиапазона)

Лазерный детектор «Антижучок»

Измерительная аппаратура:

Осциллограф RIGOL DS1202Z-E

Шумомер «Октава-110А»

Ход работы

1. Тестирование акустических помех

1.1. Ультразвуковое подавление

Разместите диктофон в 1 м от излучателя

Подайте сигналы:

19 кГц (порог слышимости)

22 кГц (оптимальное воздействие)

Оцените качество записи:

Частота	Уровень сигнала	Эффект подавления
---------	-----------------	-------------------

19 кГц	90 дБ	Частичный
--------	-------	-----------

22 кГц	105 дБ	Полный
--------	--------	--------

1.2. Инфразвуковое воздействие

Установите генератор на 12 Гц

Проверьте:

Вибрацию корпуса (акселерометром)

Уровень искажений в записи

2. Проверка детекторов

2.1. RF-сканирование

Включите радиодиктофон

Просканируйте диапазон:

400–470 МГц (аналоговые устройства)

2.4 ГГц (цифровые системы)

2.2. Лазерное детектирование

Направьте луч на:

Микрофонный узел

Светодиоды индикации

Фиксируйте отраженный сигнал

Оформление результатов

1. Сравнительная таблица эффективности

Метод подавления	Диапазон	Дальность	Время воздействия
Ультразвук 22 кГц	18–24 кГц	3 м	2–5 сек
Инфразвук 12 Гц	5–19 Гц	1.5 м	10–15 сек

2. Рекомендации по защите

Для переговорных комнат:

Комбинированные излучатели (УЗ+ИЗ)

Многослойные акустические панели

Для мобильной защиты:

Карманные подавители

Детекторы с NFC-сканированием

Вопросы для защиты

1. Почему ультразвук эффективнее подавляет цифровые диктофоны?
2. Какие физические ограничения у инфразвукового метода?
3. Как обойти защиту с помощью направленных микрофонов?
4. Какие новые технологии записи устойчивы к помехам?

Лабораторная работа 11 защита от утечки информации через тепловые каналы

Цель работы:

Проведение комплексного термографического исследования электронных устройств для выявления информационных тепловых следов.

Разработка и тестирование эффективных методов маскировки тепловых излучений.

1. Теоретическая часть

1.1. Физические основы тепловой утечки

Тепловое излучение электронных устройств содержит информационные следы благодаря:

Динамике нагрева/охлаждения компонентов (коррелирует с выполняемыми операциями)

Остаточному теплу после ввода данных (клавиатуры, сенсорные экраны)

Тепловым паттернам на дисплеях (сохраняются после выключения)

1.2. Критичные элементы устройств

Компонент	Информационная угроза	Типичная ΔT
Клавиатура	Последовательность нажатий клавиш	2-5°C
ОЗУ	Остаточный нагрев ячеек памяти	3-7°C
CPU/GPU	Характер нагрузки (шифрование/графика)	10-20°C
ЖК-дисплей	Контурь последнего изображения	1-3°C

1.3. Методы термографического анализа

Статическая термография (FLIR Tools):

Разрешение: 160×120 пикселей

Точность: ±2% от показаний

Динамический мониторинг (ThermoVision):

Частота съемки: 30 Гц

Анализ градиентов нагрева

2. Экспериментальная часть

2.1. Подготовка оборудования

Измерительный комплекс:

Тепловизор FLIR E8 (чувствительность 0.03°C)

Климатическая камера (стабилизация фона 23±0.5°C)

Эталонный излучатель (Черное тело 30°C)

Испытуемые устройства:

Ноутбук ASUS ROG (i7-11800H, RTX 3060)

Механическая клавиатура Logitech G913

Смартфон Samsung Galaxy S22 Ultra

2.2. Методика измерений

Эксперимент 1. Анализ клавиатурного ввода

Условия:

Температура фона: 23°C

Влажность: 45%

Процедура:

python

```
for _ in range(10):
```

```
    print("Пароль: 7H9s!kLp") # Ввод конфиденциальных данных
```

```
    sleep(2)
```

Параметры съемки:

Дистанция: 0.5 м

Частота кадров: 10 Hz

Результаты:

Клавиша	Макс ΔT	Время релаксации
---------	-----------------	------------------

7	+4.2°C	210 сек
---	--------	---------

H	+3.9°C	195 сек
---	--------	---------

!	+5.1°C	240 сек
---	--------	---------

Эксперимент 2. Тепловые следы дисплея

Тестовое изображение: QR-код с конфиденциальными данными

Протокол:

Экспозиция: 5 мин

Выключение дисплея → съемка через 0/2/5 мин

Данные:

Время после выключения	Видимость QR-кода
------------------------	-------------------

0 мин	100%
-------	------

Время после выключения	Видимость QR-кода
------------------------	-------------------

2 мин	75%
-------	-----

5 мин	30%
-------	-----

2.3. Методы защиты

Тест 1. Терморассеивающие покрытия

Материалы:

Графеновая пленка (толщина 50 мкм)

Керамическое напыление ZrO_2

Результаты:

Покрытие	Эффективность маскировки	ΔT клавиш
----------	--------------------------	-------------------

Без защиты	0%	+4.5°C
------------	----	--------

Графен	82%	+0.8°C
--------	-----	--------

ZrO_2	91%	+0.4°C
---------	-----	--------

Тест 2. Активные системы подавления

Конфигурация:

Peltier-элементы (12 В, 5 А)

PID-регулятор температуры

Параметры:

с

```
void control_temp() {  
    setpoint = 25.0;  
    Kp = 2.5, Ki = 0.1, Kd = 0.5;  
}
```

Эффективность:

Время маскировки: <15 сек

Погрешность: $\pm 0.3^\circ\text{C}$

3. Анализ результатов

3.1. Критические уязвимости

Клавиатурный ввод:

Время восстановления последовательности: до 7 мин

Чувствительность: 0.5°C (современные тепловизоры)

Экраны:

OLED-дисплеи сохраняют паттерны дольше (8-12 мин)

ЖК-матрицы менее уязвимы (3-5 мин)

3.2. Рекомендации по защите

Для рабочих станций:

Многослойные экраны (графен + керамика)

Динамическое охлаждение клавиатуры

Для серверных:

Жидкостное охлаждение с контролем ΔT

Термомаскирующие кожухи

4. Вопросы для защиты

1. Как температура окружающей среды влияет на качество термографической съемки?
2. Почему механические клавиатуры более уязвимы, чем мембранные?
3. Какие физические ограничения имеют активные системы охлаждения?
4. Как обнаружить тепловые следы через стеклянные перегородки?

Список литературы

Основная литература:

1. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8.
2. Киренберг А. Г., Коротин В. О. Защита информации от утечки по техническим каналам : учебное пособие / Киренберг А. Г., Коротин В. О. - Кузбасский государственный технический университет имени Т. Ф. Горбачева, 2023. - ISBN 978-5-00137-407-7.
3. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие / А. А. Сидак, В. В. Василенко, С. В. Рыженко. - Москва : Директ-Медиа, 2022. - 128 с. - ISBN 978-5-4499-3327-0.
4. Методы и средства защиты акустической речевой информации от утечки по техническим каналам: лабораторный практикум : практикум / С. В. Рыженко, В. В. Василенко, А. А. Сидак. - Москва : Директ-Медиа, 2023. - 92 с. - ISBN 978-5-4499-3603-5.

Дополнительной литература:

1. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Г. А. - М. : Горячая линия - Телеком, 2016. - 585 с. : ил. - Библиогр.: с. 574-581. - ISBN 978-5-9912-0424-8.
2. Вайц Е. В., Грачёва Ю. В. Разработка комплекса организационных и технических мероприятий по защите информации от утечки по техническим каналам на объекте информатизации : методические указания к выполнению курсовой работы / Вайц Е. В., Грачёва Ю. В. ; МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2016. - 15 с. : ил. - Библиогр. в конце брош. - ISBN 978-5-7038-4556-1.
3. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / Евстифеев А. А., Ерошев В. И., Мартынов А. П. [и др.]. - Российский федеральный ядерный центр – ВНИИЭФ, 2019. - ISBN 978-5-9515-0426-5.
4. Технические средства разведки и защита информации : учебное пособие / О. Т. Данилова. - Омск : Омский государственный технический университет (ОмГТУ), 2019. - 64 с. - ISBN 978-5-8149-2839-9 (Ч. 1). - ISBN 978-5-8149-2838-2.