МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»

(Самарский университет)

Институт информатики и кибернетики

Кафедра геоинформатики и информационной безопасности

Отчет по лабораторной работе №1 по дисциплине

«Техническая защита информации»

«**ИССЛЕДОВАНИЕ НИЗКОЧАСТОТНЫХ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ВТСС И ТОКОПРОВОДЯЩИХ ЛИНИЯХ**»

Выполнили:

Журавлев С. А.

Акутин И. Д.

Овсянников А. Н.

Спиридонва К. С.

гр. 6312-100503D

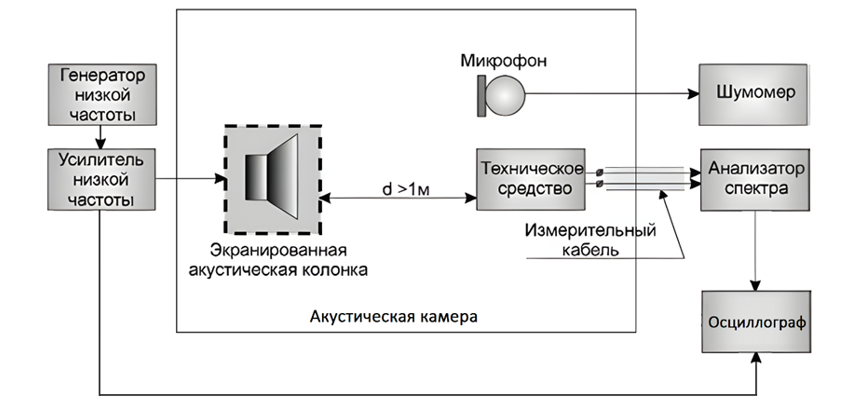
Проверил:

Хабаров Д. А.

Самара, 2024

*Цель работы:* выявление опасных сигналов, возникающих за счет низкочастотных акустоэлектрических преобразований.

*Описание установки и оборудования.*

Рисунок 1 Общая схема установки

*Расчеты.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Среднегеометрическая частота октавы *Fi*, Гц | Полоса пропускания фильтра анализатора спектра ∆*Fi*, Гц | Ширина полосы октавы ∆*Fi*, Гц | Нормированный уровень звукового давления *L*н*i*, дБ | Измеренный уровень звукового давления *Li*, дБ | Напряжение «сигнал+шум» Uсшi, дБ | Напряжение шума Uшi, дБ |
| 525 | 3 | 350 | 66 | 96 | 38 | 0 |
| 1025 | 3 | 700 | 66 | 93.3 | 38 | 0 |
| 2025 | 3 | 1400 | 61 | 87.7 | 38 | 0 |
| 4025 | 3 | 2800 | 56 | 82.3 | 38 | 0 |
| 8025 | 3 | 5600 | 53 | 78 | 38 | 0 |

Таблица 2 Результаты измерений

**2.4 Обработка результатов измерений**

Рассчитать уровень информативного сигнала:

Рассчитать степень превышения создаваемого акустического давления над нормированным звуковым давлением в i-ой октаве:

Рассчитать уровень информативного сигнала, приведенного к нормированному уровню акустического воздействия:

Рассчитать отношение "сигнал/шум":

Если для всех *i*вычисленное отношение "сигнал/шум" Δ𝑖 меньше нормированного, то это исследуемое ТС соответствует нормам противодействия в анализируемом режиме работы ТС и варианте подключения.

2.4.6. При проведении инструментального контроля нормируемым показателем (нормой противодействия) является Δi – отношение "сигнал/шум" на в каждой точке **во всех октавах** полосы речевых частот (5 октав). **За норму противодействия принимают величину Δн = 0,3**. Если Δi < Δн, (i – номер октавы) для всех октав, то норма противодействия выполняется. Результаты расчетов внести в табл. 2.4.

Таблица 2.4 – Результаты расчетов

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Среднегеометрическая частота октавы *Fi*, Гц | Измеренный уровень звукового давления *Li*, дБ | Напряжение «сигнала» Uсi, мкв | Напряжение шума *U*ш*i*, дБ | Приведенное напряжение сигнала  U(с прив i), мкВ | Отношение "сигнал/шум"  Δi |
| 525 | 96 | 79.42652859 | 0 | 2.51168737 | 0.03394172 |
| 1025 | 93.3 | 79.4265286 | 0 | 3.42740623 | 0.16719055 |
| 2025 | 87.7 | 79.4265286 | 0 | 3.67253194 | 0.79837651 |
| 4025 | 82.3 | 79.4265286 | 0 | 3.84561304 | 3.84561304 |
| 8025 | 78 | 79.4265286 | 0 | 4.46648193 | 37.2206828 |

*Контрольные вопросы*

1. **Физические основы возникновения канала низкочастотного акустоэлектрического преобразования**: Канал НЧ АЭП возникает в результате взаимодействия звуковых волн с электрическими полями в средах, таких как полупроводники. При этом акустические волны могут вызывать изменения в электрических свойствах материала, что приводит к генерации электрического сигнала. Это явление объясняется эффектом пьезоэлектричества, когда механическое воздействие на материал приводит к возникновению электрического заряда.
2. **ВТСС в защищаемом помещении, которые должны исследоваться на наличие канала НЧ АЭП**: В защищаемом помещении следует исследовать все виды вычислительной и офисной техники, включая компьютеры, принтеры, телефоны и системы связи. Эти устройства могут быть источниками или приемниками акустических сигналов, которые злоумышленник может использовать для утечки информации.
3. **Варианты подключения к ВТСС для формирования технического канала утечки речевой информации**: Злоумышленник может использовать следующие варианты подключения:
   * Прямое подключение к аудиовыходам или микрофонам устройств.
   * Использование беспроводных технологий (например, Bluetooth) для доступа к устройствам.
   * Установка скрытых микрофонов или других записывающих устройств вблизи защищаемого оборудования.
4. **Нормируемые показатели противодействия**: К нормируемым показателям могут относиться:
   * Уровень шума в защищаемом помещении.
   * Чувствительность используемых устройств к акустическим сигналам.
   * Эффективность систем защиты информации (например, шифрования).
5. **Физическая сущность методики по выявлению канала утечки речевой информации, обусловленного НЧ АЭП**: Методика включает в себя анализ акустических свойств помещений и устройств, мониторинг электромагнитных излучений и оценку уровня утечки информации через акустические каналы. Это может включать в себя использование специализированного оборудования для записи и анализа звуковых сигналов.
6. **Средства измерений для выявления канала утечки, обусловленного НЧ АЭП**: Для выявления канала утечки могут использоваться:
   * Акустические анализаторы.
   * Осциллографы для анализа сигналов.
   * Специальные микрофоны и записывающее оборудование для мониторинга звуковых волн.
7. **Порядок проведения измерений в канале НЧ АЭП**: Измерения проводятся в несколько этапов:
   * Подготовка помещения и оборудования.
   * Проведение предварительного аудита и оценки акустических характеристик.
   * Измерение уровней звуковых сигналов и их анализ.
   * Сравнение полученных данных с нормируемыми показателями.
8. **Физическая сущность расчетов, проводимых по результатам измерений**: Расчеты основаны на анализе полученных данных для определения степени утечки информации. Это может включать в себя статистическую обработку измеренных сигналов, оценку их амплитуды и частоты, а также сравнение с эталонными значениями.
9. **Организационно-технические меры для закрытия канала, обусловленного НЧ АЭП**: Меры могут включать:
   * Установку акустических барьеров и звукоизоляции.
   * Использование специализированных фильтров для подавления нежелательных сигналов.
   * Регулярный аудит и тестирование систем на наличие уязвимостей.