

Практическая работа 3: Оценка защищенности помещений от утечки информации по электромагнитному каналу

Тема: Оценка защищённости защищаемого помещения от утечки информации по электромагнитному каналу утечки информации.

Цель: Определить, возможна ли утечка конфиденциальной информации по электромагнитному каналу.

Описание: Данная практика позволит укрепить навыки расчётов параметров электромагнитного поля и электромагнитных сигналов.

Оборудование:

- Исходные данные
- Программа создания электронных таблиц (Excel, Google Таблицы)
- Математические пакеты (например, Desmos, matplotlib)

Задачи:

1. Изучить исходные данные
2. Определить частоты гармоник и их интервалы
3. Вычислить напряженность поля на границе КЗ
4. Определить отношение «сигнал/помеха» и сделать выводы

Описание работы

В данной работе будет рассматриваться помещение с компьютером, на котором обрабатывается конфиденциальная информация.

Даже не имея доступа в помещение и не имея возможности подсмотреть или подслушать обрабатываемую информацию, злоумышленник может попытаться её считать. Это возможно из-за того, что работающие части компьютера — например, монитор или жесткий диск — излучают паразитные электромагнитные волны, которые могут быть перехвачены и обработаны.

Эти электромагнитные волны, известные как побочные электромагнитные излучения и наводки (ПЭМИН), могут содержать информацию о данных, обрабатываемых компьютером. Злоумышленники могут использовать специализированное оборудование для перехвата и анализа этих волн, пытаясь декодировать информацию. Это одна из причин, почему важно обеспечивать электромагнитную защиту для компьютеров и других устройств, обрабатывающих конфиденциальную информацию.

В этой работе не будет описания способов съема информации, содержащейся в ПЭМИН. Вместо этого будет рассмотрен способ определения того, достаточен ли уровень защиты системы для противодействия такой разведке.

Канал утечки ПЭМИН (как и другие каналы утечки) подвержен влиянию факторов помех, которые искажают полезный информативный сигнал. Наличие помех в сигнале усложняет восприятие сигнала. Однако, стоит иметь в виду, что у злоумышленника может быть устройство для подавления помех. Кроме того, он будет искать способы их уменьшения, например, размещая устройство ближе к границе контролируемой зоны.

Показателем качества канала утечки является отношение сигнал/помеха на входе приемника перехвата злоумышленника. Он характеризует, насколько больше в сигнале информативной части, чем помехи.

Ход работы

1. Создайте лист для вычислений.

В вашем документе — электронной таблице создайте новый лист «Электромагнитный канал». В нём будет создан модуль для расчёта защищённости здания от электромагнитного канала утечки информации.

2. Рассчитайте тактовую частоту излучения мониторов.

Экраны (дисплеи) объектов «А», «Б» и «В» излучают электромагнитные волны, распространяющиеся в среде в том числе за пределы контролируемой зоны. Чтобы узнать тактовую частоту (частоту первой гармоники) этих волн, необходимо использовать формулу:

$$F_{\text{такт.}} = N_{\text{вер.}} * N_{\text{гор.}} * F_{\text{к}} * \frac{kx}{q}$$

Где:

- $N_{\text{вер.}}$ — количество пикселей по вертикали;
- $N_{\text{гор.}}$ — количество пикселей по горизонтали;
- $F_{\text{к.}}$ — частота обновления монитора (Гц);
- k — коэффициент учёта обратного хода луча;
- x — коэффициент развёртки;
- q — коэффициент тестового сигнала.

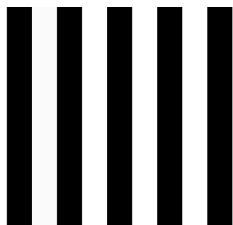
Первые три параметра являются исходными данными, их значения находятся на листе «Исходные данные».

Коэффициент учёта обратного хода луча, как правило, находится в диапазоне 1,1...1,5. Данный коэффициент позволяет учитывать время, затрачиваемое на строчный и кадровый синхроимпульсы, которые обеспечивают обратный ход электронного луча кинескопа. Современные ЖК-экраны не имеют электронно-лучевых кинескопов, однако, стандарты аналогового телевидения существуют в неизменном виде для возможности приёма телепрограмм всеми телевизорами, в том числе с кинескопом. В этой работе принимайте для всех объектов $k = 1,2$. У более старых мониторов этот коэффициент выше.

Коэффициент развёртки равен 1 для прогрессивной развёртки (когда все строки каждого кадра отображаются последовательно) и равен 2 для чересстрочной развёртки (когда чётные и нечётные строки отображаются отдельно, что было характерно для телевизоров с электронно-лучевой трубкой). Для объектов «Б» и «В»

примите $x = 1$. Скорее всего, ваш компьютер также имеет современный ЖК-экран, поэтому для объекта «А» также примите $x = 1$.

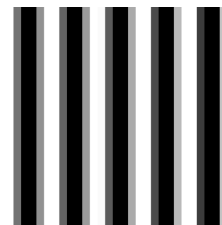
Коэффициент тестового сигнала зависит от вида монитора в тестовом режиме. Ниже приведены основные разновидности тестового сигнала:



точка-через-точку



строчка-через-строчку



столбец-через-столбец

В данной работе будет использоваться режим «точка-через-точку», при котором уровень излучаемых ПЭМИН максимален. В этом режиме $q = 2$.

Занесите тактовые частоты для каждого объекта в Excel.

3. Рассчитайте длительность тестового и единичного импульсов.

Для каждого объекта защиты рассчитайте длительность импульса тестового сигнала и длительность единичного импульса, используя формулы.

Длительность импульса тестового сигнала:

$$T_{\text{и}} = \frac{1}{F_{\text{такт.}}}$$

Длительность единичного импульса:

$$\tau_{\text{и}} = \frac{T_{\text{и}}}{2}$$

Занесите эти данные в Excel.

4. Создайте модуль для расчёта частот других гармоник.

Если бы монитор излучал только сигналы на тактовой частоте, то он бы отображал лишь монотонную одноцветную картинку. В реальности же излучаемые сигналы содержат частоты более высоких гармоник. Таких гармоник может быть много, однако, самыми информативными можно считать первые десять нечётных гармоник.

Создайте на вашем листе пустую таблицу подобного формата:

Частоты для 10 гармоник		Расчёт интервалов		
Гарм-ка	Частота, МГц	Интервал	f_ниж, МГц	f_верх, МГц
1		i_1 =		
3		i_3 =		
5		i_5 =		
7		i_7 =		
9		i_9 =		
11		i_11 =		
13		i_13 =		
15		i_15 =		
17		i_17 =		
19		i_19 =		

Выберите объект с самой маленькой длительностью импульса тестового сигнала и заполните таблицу для него.

Частота первой гармоники равна тактовой частоте, которая была рассчитана на втором шаге. Частоты остальных гармоник вычисляются как произведение тактовой частоты на номер гармоники:

$$F_j = F_{\text{такт.}} * j$$

Номер интервала рассчитывается по следующей формуле:

$$i_j = \lfloor 1 + F_j * \tau_{\text{и}} \rfloor$$

В этой формуле либо используйте систему СИ (то есть F_j подставляйте в Гц, а $\tau_{\text{и}}$ в с), либо используйте МГц и мкс. Если вы всё сделали правильно, номера интервалов должны быть от 1 до 10. Для вычисления функции антье (округления вниз) используйте функцию Excel ОКРВНИЗ.

Для расчёта нижней и верхней границы интервала используйте формулы:

$$F_{i_{\text{нижн.}}} = \frac{i - 1}{\tau_{\text{и}}}$$

$$F_{i_{\text{верх.}}} = \frac{i}{\tau_{\text{и}}}$$

5. Постройте временной график и спектрограмму сигнала.

Чтобы построить графики сигнала, воспользуйтесь специальными математическими программами и пакетами (например, *Desmos*) или используйте библиотеки для языков программирования (например, *matplotlib* для *Python*).

Пример кода на Python:

```
import numpy as np
import matplotlib.pyplot as plt

time = np.linspace(0, 1, 1000)
A = [1.4, 0.35, 0.15, 0.1, 0.09, 0.08, 0.07, 0.06, 0.05, 0.04] # Амплитуды
f = [11.1, 33.2, 55.3, 77.4, 99.5, 121.6, 143.8, 165.9, 188.0, 210.1] # Частоты
signal = [0] * 10
signal[0] = A[0] * np.sin(2 * np.pi * f[0] * time)
signal[1] = A[1] * np.sin(2 * np.pi * f[1] * time)
signal[2] = A[2] * np.sin(2 * np.pi * f[2] * time)
signal[3] = A[3] * np.sin(2 * np.pi * f[3] * time)
signal[4] = A[4] * np.sin(2 * np.pi * f[4] * time)
signal[5] = A[5] * np.sin(2 * np.pi * f[5] * time)
signal[6] = A[6] * np.sin(2 * np.pi * f[6] * time)
signal[7] = A[7] * np.sin(2 * np.pi * f[7] * time)
signal[8] = A[8] * np.sin(2 * np.pi * f[8] * time)
signal[9] = A[9] * np.sin(2 * np.pi * f[9] * time)
signal = sum(signal)

spectrum = np.fft.fft(signal) / len(signal) * 2
freq = np.fft.fftfreq(len(signal), 1 / len(signal))

plt.figure(figsize=(10, 8))
plt.subplot(4, 1, 1)
plt.plot(time, signal)

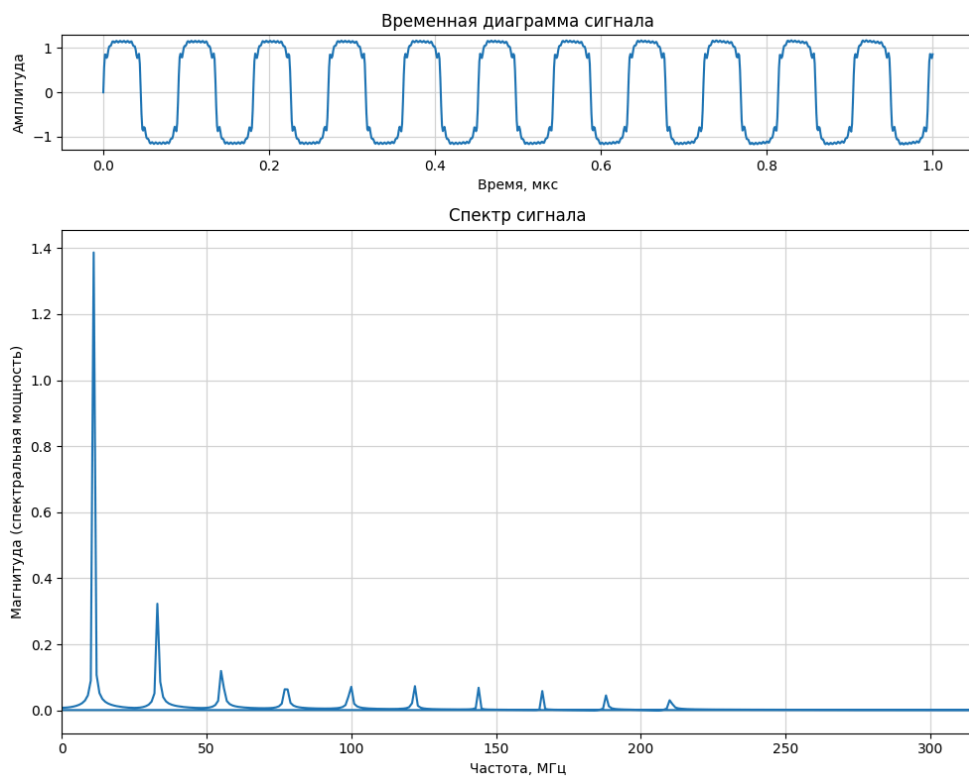
plt.xlabel('Время')
plt.ylabel('Амплитуда')
plt.title('Временная диаграмма сигнала')
plt.grid(True, color='lightgray')

plt.subplot(4, 1, (2, 4))
plt.plot(freq, np.abs(spectrum))
plt.xlim(0, f[9] * 1.5)
plt.xlabel('Частота')
plt.ylabel('Магниту́да (спектральная мощность)')
plt.title('Спектр сигнала')

plt.tight_layout()
plt.grid(True, color='lightgray')

plt.show()
```

Эмпирически подберите такие значения амплитуд, чтобы сигнал выглядел как последовательность прямоугольных видеоимпульсов (как на рисунке ниже), с амплитудой, примерно равной 1.



Если вы всё сделали правильно, «пики» спектра сигнала будут располагаться на тех частотах, которые были рассчитаны во втором столбце таблицы гармоник (Частота).

Вставьте в отчёт временную диаграмму и спектр сигнала.

6. Выберите частоты для исследования.

Для дальнейших расчётов необходимо взять три частоты, для которых будут определены напряжённости электромагнитного поля, создаваемого компьютерами, а затем вычислены параметры «сигнал/помеха». Создайте в Excel таблицу:

Параметр	Частота		
	100 МГц	500 МГц	1000 МГц
(Е) Напряженность поля
...

Напряжённость поля на частотах 100 МГц и 500 МГц указана в практике № 0 в таблице вариантов (E_{100} и E_{500}).

Напряжённость поля на частоте 1000 МГц определите как $E_{500} - 10$ мкВ/м, если номер вашего варианта чётный, либо $E_{500} + 10$ мкВ/м, если номер вашего варианта нечётный.

Результаты запишите в таблицу.

7. Рассчитайте напряжённость поля на границе контролируемой зоны.

Напряжённость электромагнитного поля постепенно снижается с расстоянием. Этому способствуют два фактора: естественное затухание поля с расстоянием и экранирование поля стеной здания. Нужно учесть оба этих фактора, чтобы рассчитать напряжённость поля у границы контролируемой зоны.

Коэффициент затухания находится по формуле:

$$k_{\text{затухания}} = \frac{1}{r^n}$$

где: r — расстояние от источника ПЭМИН до границы КЗ

n — показатель затухания волн

Оба этих аргумента находятся на листе «Исходные данные» вашей таблицы.

Коэффициент экранирования определяется экспериментально: для этого специальным прибором измеряют напряжённость поля перед ограждением и за ним, а затем находят их отношение. Чтобы упростить задачу, коэффициенты экранирования некоторых наиболее часто используемых ограждающих конструкций сведены в таблицу:

Тип здания	Коэффициент экранирования $k_{\text{экр}}$ на частотах		
	100 МГц	500 МГц	1000 МГц
Деревянное здание (с толщиной стен 20 см)			
окно без решётки	1,8 — 2,2	2,2 — 2,8	2,8 — 3,5
окно закрыто решеткой с ячейкой 5 см	2,0 — 2,5	3,2 — 4,0	4,0 — 5,0
Кирпичное здание (с толщ. стены 1,5 кирпича)			
окно без решётки	4,5 — 5,6	5,6 — 7,0	6,3 — 8,9
окно закрыто решеткой с ячейкой 5 см	7,0 — 8,9	10,0 — 12,6	12,6 — 17,8
Железобетонное здание (с толщ. стены 160 мм)			
окно без решётки	10,0 — 17,8	8,0 — 8,9	5,6 — 7,0
окно закрыто решеткой с ячейкой 5 см	25,1 — 39,8	14,1 — 22,4	10,0 — 17,8

Зрительно оцените, из какого материала сделаны стены здания вашего варианта. Если этот материал есть в таблице выше, возьмите соответствующие коэффициенты экранирования из неё (поскольку в ячейках даны диапазоны, возьмите для расчётов максимальное значение диапазона). Если материала нет в таблице, считайте, что его коэффициент экранирования такой же, как и у деревянного здания с толщиной стен 20 см.

Зная коэффициент затухания и коэффициент экранирования, можно определить напряженность поля на границе контролируемой зоны, где находится злоумышленник:

$$E_{\text{к.з.}} = E * \frac{k_{\text{затухания}}}{k_{\text{экранирования}}}$$

8. Рассчитайте напряжённость поля атмосферных помех.

Атмосферные помехи всегда присутствуют в окружающем пространстве, они обусловлены электрическими процессами в атмосфере, прежде всего грозовыми разрядами. Они вносят искажение в информативный сигнал ПЭМИН, что усложняет нарушителю задачу расшифровки сигнала. Напряжённость поля атмосферных помех рассчитывается по формуле:

$$E_{\text{атм.}} = 10 \lg\left(\frac{T_a}{T_o}\right) - 65.5 + 20 \lg(f) + 10 \lg(f_{\text{экв.}})$$

где: T_a — эквивалентная шумовая температура, характеризующая интенсивность помех (принимается за 293 К)

T_o — опорный уровень шумовой температуры (273 К)

f — частота, МГц

$f_{\text{экв}}$ — ширина полосы пропускания приемника (принимается за 40 МГц)

Данная формула выдает результат в децибелах. Чтобы перевести их в мкВ/м, необходимо воспользоваться формулой:

$$E_{\text{атм.}} [\text{мкВ/м}] = 10^{\frac{E_{\text{атм.}} [\text{дБ}]}{20}}$$

Рассчитайте напряжённость поля атмосферных помех для трёх частот из предыдущего шага.

9. Вычислите отношение «сигнал/помеха».

Вычислите отношение информативного сигнала к сигналу атмосферных помех на границе контролируемой зоны для каждой частоты:

$$\Delta = \frac{E_{\text{к.з.}}}{E_{\text{атм.}}}$$

10. Подготовьте рекомендации по обеспечению защиты.

Сравните значения с требуемым и рекомендуемым значениями, которые даны в таблице ниже:

Параметр	Объект защиты			
	А	Б	В	Г
$\Delta_{\text{требуемое}}$	0,7	1	1	1
$\Delta_{\text{рекомендуемое}}$	0,5	0,8	0,9	0,9

Если ваши значения выше требуемого, то необходимо принять меры по обеспечению более высокого уровня защиты помещения. Укажите их в отчёте — например, переместить ПК в другое помещение, дальше от границ контролируемой зоны, увеличить толщину стены, поставить решётки на окна и т.д.

Если ваши значения ниже требуемого, но выше рекомендуемого, то также рекомендуется принять некоторые меры по обеспечению дополнительной защиты помещения. В этом случае укажите в отчёте, что в отношении данного объекта защиты необходимо задуматься о повышении его защиты.

Если ваши значения ниже рекомендуемого, то дополнительных рекомендаций не требуется.

Проделайте эти сравнения для каждого объекта защиты и для каждого объекта приведите рекомендации (если требуется).

11. Оформите вывод по проделанной работе.

В выводе укажите, у каких объектов выполняются или не выполняются требования по защите информации от утечки по электромагнитному каналу. На основании этого составьте прогноз, какую информацию нарушитель может получить путём перехвата и анализа ПЭМИН (исходя из описания и назначения объектов защиты).

Контрольные вопросы

Основные вопросы.

1. Приведите определение электромагнитных каналов утечки информации
2. Что такое ПЭМИН? Какова природа его возникновения?
3. Для чего нужен спектральный анализ сигнала?
4. Что такое атмосферные помехи?
5. Что такое отношение «сигнал/шум»? Как оно характеризует степень защиты?
6. Что такое экранирование? Что показывает коэффициент экранирования?

Бонусные вопросы.

1. Что такое строчный и кадровый синхроимпульсы?
2. Какие уравнения используются для расчета электромагнитного поля?
3. Что такое аддитивные помехи? Приведите примеры аддитивных помех (кроме атмосферных)
4. Что такое паразитные наводки и паразитные связи?
5. Какие методы существуют для защиты от электромагнитных каналов утечки информации?
6. Каковы основные принципы работы экранирования от электромагнитных помех?