Практическая работа 4: Утечка информации по линиям связи

Тема: Оценка защищённости защищаемого помещения от утечки информации по линиям связи.

Цель: Определить, возможна ли утечка конфиденциальной информации по линии телефонной связи.

Описание: В этой практике будут рассмотрены различные способы прослушивания телефонного канала связи.

Оборудование:

1. План и схемы защищаемого помещения
2. Программа создания электронных таблиц (Excel, Google Таблицы)
3. Математические пакеты (например, Desmos, matplotlib)

Задачи:

1. Создать амплитудно-модулированный сигнал
2. Провести спектральный анализ сигнала
3. Получить информативный сигнал

Описание работы

Когда информация передается по линиям связи, электрический канал утечки может возникнуть, если кабели подключаются непосредственно к устройствам перехвата. Чтобы сделать этот процесс скрытым, устройства перехвата подключаются к линии через специальные устройства, которые снижают сопротивление и напряжение на линии. Некоторые кабели связи имеют воздухонепроницаемую оболочку, которая создает избыточное давление внутри. В таком случае, устройства перехвата должны быть способны компенсировать снижение давления воздуха при подключении к кабелю.

Этот метод наиболее часто используется для перехвата низкочастотных телефонных сигналов на общедоступных участках линий связи. Затем перехваченная информация может быть записана на диктофон или передана по радиоканалу. Если такие устройства содержат радиопередатчики для передачи перехваченной информации, их называют телефонными закладками.

Один из основных способов незаконного доступа к частной и коммерческой информации — это прослушивание телефонных разговоров. Для прослушивания телефонных разговоров используются следующие способы подключения:

— Параллельное подключение к линии связи. В этом случае сложнее обнаружить телефонные устройства для прослушивания, но для их работы требуется внешний источник питания.
— Последовательное подключение телефонных устройств для прослушивания к разорванной линии связи. В этом случае питание телефонного устройства осуществляется от самой линии связи, и оно начинает передачу с момента, когда абонент поднимает трубку.

Ход работы

1. Создайте лист для вычислений.

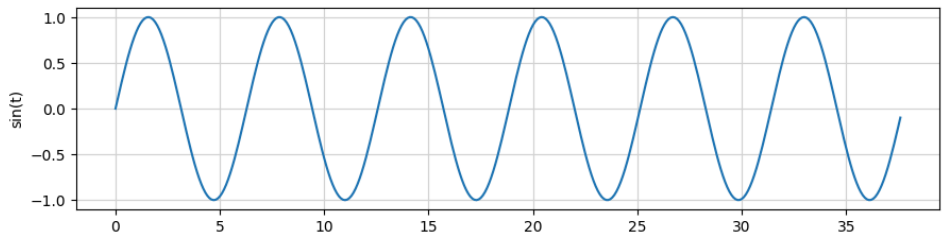
В вашем документе — электронной таблице создайте новый лист «Линии связи». В нём будет создан модуль для расчёта защищённости здания от утечки информации по линиям связи.

Среди ваших объектов защиты только один телефонный аппарат (объект «Г»), поэтому вся работа будет связана только с ним. Объекты «А», «Б», «В» и «Д» в этой работе принимать участие не будут.

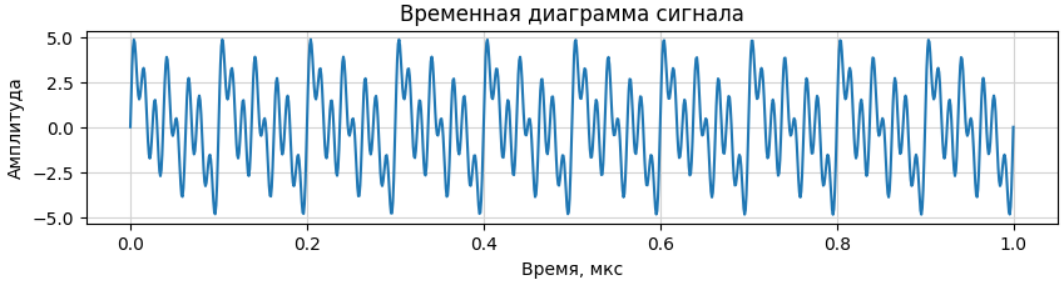
2. Придумайте информативный сигнал.

Вся информация, передающаяся по проводам, является электрическим сигналом. Сигнал можно рассматривать как функцию, переносящую информацию о поведении физической системы.

Пример простого сигнала — функция синуса *f(t)=sin(t)*.



Однако, сигнал чистого синуса малоинформативен. Обычно сигнал является суммой нескольких элементарных сигналов разных частот и амплитуд:



Создайте свой сигнал из суммы отдельных синусоидальных сигналов на основании вашего имени и фамилии:

1. Возьмите свое имя и фамилию.
2. Расположите буквы в алфавитном порядке.

3. Присвойте каждой букве два значения: амплитуда и частота. Амплитуда равна количеству повторяющихся букв. Частота определяется как номер буквы в последовательности (без учёта повторений), умноженный на ваш номер в списке студентов.
4. Если вы получили больше 10 частот, используйте только первые 10.

Например, предположим, что ваше имя и фамилия — «Джессика Локк», и вы являетесь 3-м студентом в списке.

1. Первым шагом будет упорядочение букв: "АДЕЖИКККЛОСС".
2. Затем мы присваиваем каждой букве амплитуду (количество повторений) и частоту (номер в последовательности, умноженный на ваш номер в списке): А(1,3), Д(1,6), Е(1,9), Ж(1,12), И(1,15), К(3,18), Л(1,21), О(1,24), С(2,27).
3. Получаем следующую таблицу частот и сигналов:

f	3	6	9	12	15	18	21	24	27
A	1	1	1	1	1	3	1	1	2

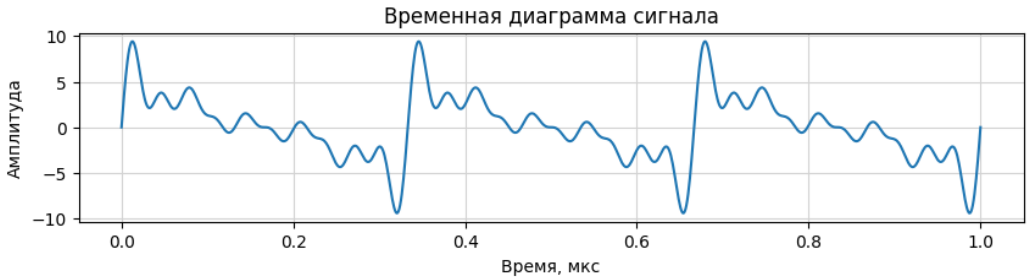
Сформируйте ваш сигнал:

$$A(t) = \sum_{i}^{N} (A_i \sin(2\pi f_i t))$$

Постройте график вашего сигнала (для этого можно использовать математические пакеты, такие как matplotlib для Python).

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

time = np.linspace(0, 1, 1000)
f = [1, 2, 3, 4] # Частоты
A = [1, 1, 1, 1] # Амплитуды
signal = np.zeros(1000)
for i in zip(A, f):
    signal += i[0] * np.sin(2 * np.pi * i[1] * time)

plt.figure(figsize=(10, 2))
plt.plot(time, signal)

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

plt.show()
```

Пример графика сигнала:



Данный график представляет конфиденциальную информацию (например, аудиосигнал конфиденциальных переговоров). Дальнейшие шаги будут симулировать то, как нарушитель может попытаться получить этот сигнал.

Вставьте график в отчёт.

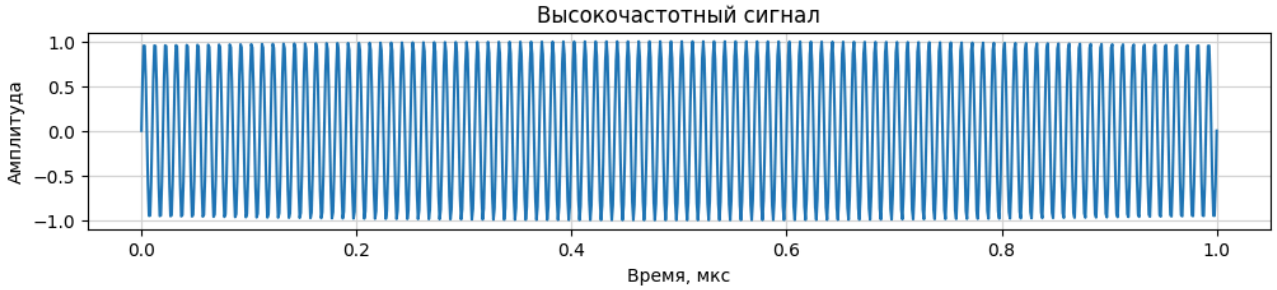
3. Протестируйте метод перехвата с помощью «микрофонного эффекта».

В комнате, где ведутся конфиденциальные переговоры, стоит телефонный аппарат (объект «Г»), трубка которого опущена (то есть микрофон телефона не работает).

Злоумышленник, если он знает топологию проводной сети, может подключить к одному из проводов телефонной линии подключить генератор высокочастотных колебаний, а к другому — амплитудный детектор с усилителем. Данный способ перехвата информации основан на «микрофонном эффекте».

«Микрофонный эффект» — это явление, при котором некоторые электронные компоненты, такие как конденсаторы и полупроводниковые устройства, начинают работать как микрофоны. Это происходит из-за того, что эти компоненты способны преобразовывать звуковые вибрации в электрический сигнал, по-прежнему сохраняя свои основные функции.

Сгенерируйте в вашей модели любой высокочастотный сигнал, частота которого примерно в 1,5–2 больше частоты вашего информативного сигнала. Например, ниже представлен сигнал частотой в 100 Гц.



Высокочастотные колебания проходят через микрофон или элементы телефонного аппарата, обладающие «микрофонным эффектом», и модулируются акустическими сигналами прослушиваемого помещения.

Сгенерируйте амплитудно-модулированный информативным сигналом высокочастотный синал. Коэффициент модуляции *m* примите за 0,9.

$$u_{am}(t) = u_c(t) * (1 + m\frac{u_m(t)}{|u_m(t)|_{max}})$$

Пример кода на Python:

```
freq_carrier = 100
carrier_signal = 1 * np.sin(2 * np.pi * freq_carrier * t)
m = 0.9
max_value = max(max(modulating_signal), -min(modulating_signal))
output_signal = (1 + m * modulating_signal / max_value) * carrier_signal
```

Это позволяет переносить информацию модулирующего сигнала через несущий сигнал. Информацию при этом несёт именно модулирующий сигнал, а несущий выступает лишь средой передачи.

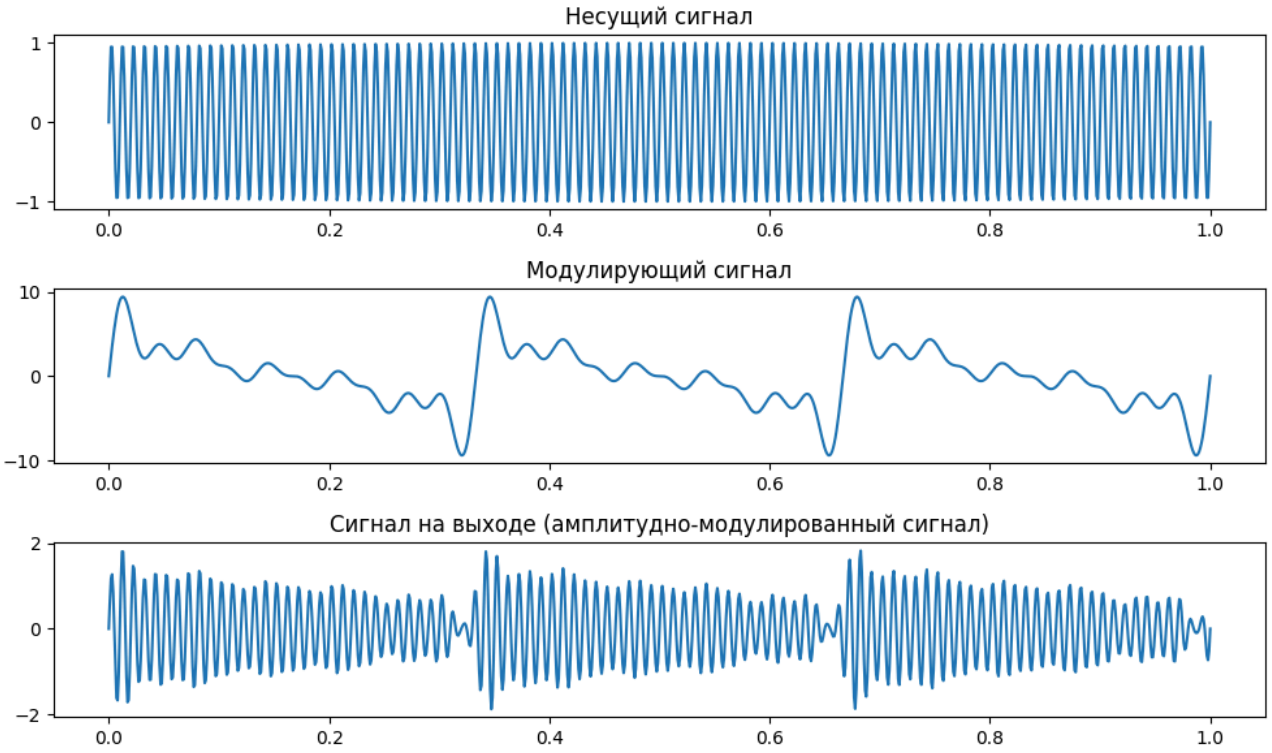


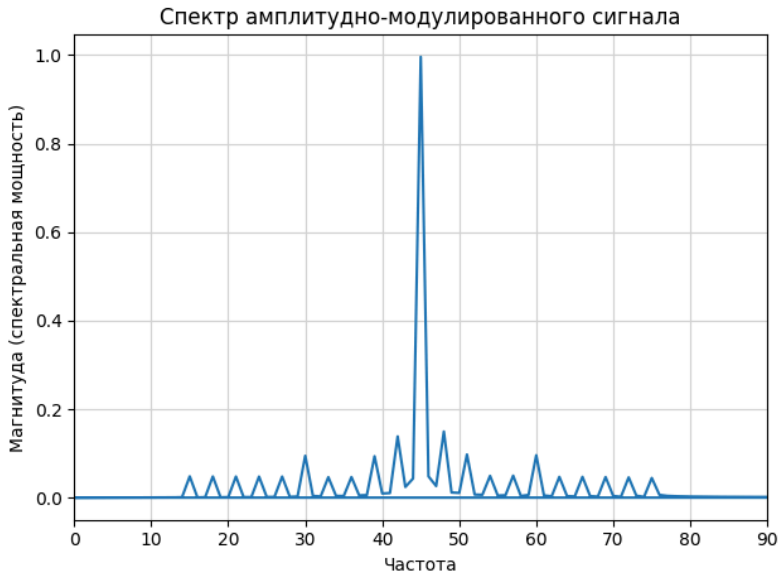
Рисунок выше наглядно показывает метод утечки. На верхней диаграмме — подаваемый нарушителем на телефонный провод высокочастотный сигнал. На

средней картинке — информативный сигнал (конфиденциальные переговоры). На нижней картинке — модулированный сигнал, который злоумышленник снимает со второго телефонного провода детектором.

Теперь его задача — восстановить информативный сигнал. Для этого необходимо построить спектр сигнала при помощи преобразования Фурье:

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

plt.plot(freq, np.abs(spectrum))
plt.xlim(0, freq_carrier * 2)
plt.xlabel('Частота')
plt.ylabel('Магнитуда (спектральная мощность)')
plt.title('Спектр амплитудно-модулированного сигнала')

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

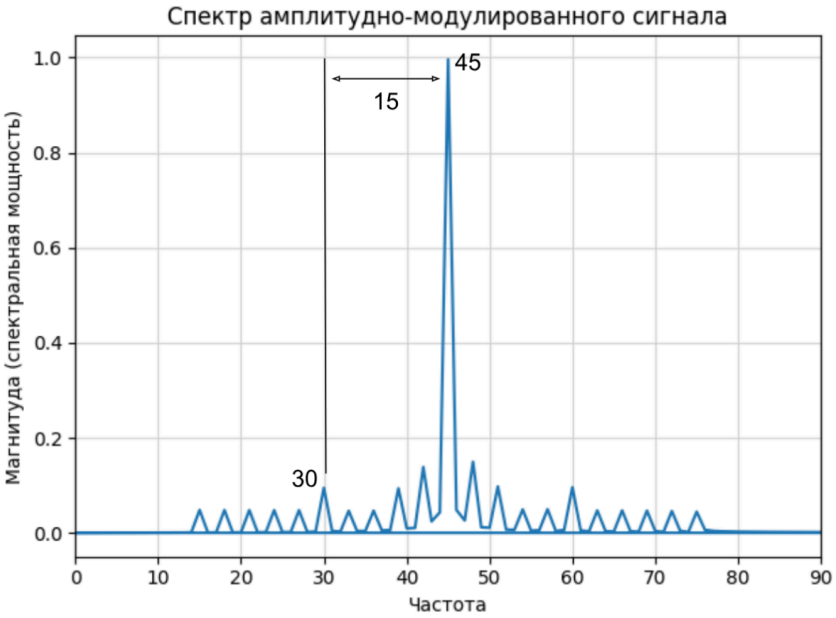
На спектре отчётливо видны составляющие сигнала:



Центральный пик — компонента несущей частоты. Остальные гармоники (называемые боковыми) располагаются парами и отвечают за информативный сигнал. Как видно, гармоники располагаются через равные промежутки (поскольку частоты распределены равномерно) и имеют разную высоту (в зависимости от амплитуды).

Составьте по спектру таблицу частот и амплитуд. Чтобы найти частоту сигнала гармоники, найдите разницу между частотой центральной гармоники и частотой конкретной боковой гармоники.

Пример измерения частоты гармоники сигнала:



Если вы всё сделали правильно, у вас должна получиться таблица информативного сигнала (из шага 2), что означает, что нарушитель смог получить информативный сигнал.

Скорее всего, амплитуды исходного и полученного сигналов не совпадают — это нормально, главное, чтобы они были пропорциональными. Амплитуды показывают мощность сигнала, а нарушитель может воспользоваться усилителем для увеличения амплитуды. Найдите такое число, которое при умножении на каждое число из второго набора даёт соответствующее число из первого набора.

4. Оформите вывод по проделанной работе.

В выводе укажите возможность перехвата конфиденциальной информации по линии телефонной связи.

Контрольные вопросы

Основные вопросы.

1. Какова природа возникновения канала утечки информации по линиям связи?
2. Какие типы каналов утечки информации по линиям связи существуют?
3. Каким образом возможен перехват информации путём высокочастотного навязывания?
4. Что такое «микрофонный эффект»?
5. В чём отличие параллельного подключения к линии связи от последовательного?
6. Что такое амплитудная модуляция сигнала?
7. Для чего используется спектральный анализ сигнала?

Бонусные вопросы.

1. Какие технические средства могут использоваться для обнаружения и предотвращения перехвата информации?
2. Как происходит фазовая модуляция информации в канале утечки?
3. Какие методы могут быть использованы для защиты от высокочастотного навязывания?
4. Каким образом можно обнаружить аппаратные устройства, установленные для перехвата информации на линиях связи?
5. Как влияет длина кабеля на возможность возникновения канала утечки информации?