Практическая работа 2: Выявление технических каналов утечки информации

Тема: Выявление возможных технических каналов утечки информации для выбранного здания.

Цель: Определить, через какие технические каналы возможна утечка конфиденциальной информации, которая обрабатывается в здании.

Описание: Практика посвящена обзору технических каналов утечки информации и составлению перечня исходных данных.

Оборудование:

- Схема выбранного здания
- Фотоматериал (фотографии здания)
- Программа создания электронных таблиц (Excel, Google Таблицы)
- Картографические сервисы (Яндекс.Карты, Google Maps)
- Графический редактор (draw.io, Illustrator, Inkscape)

Задачи:

1. Изучить план и схемы выбранного здания.
2. Определить объекты защиты.
3. Определить характеристики и параметры объектов защиты.
4. Составить описание возможных каналов утечки информации.
5. Составить схемы одного из каналов утечки информации

Описание работы

Эта работа является предисловием для ряда следующих работ, в которых исследуется каждый канал утечки информации по отдельности.

Технический канал утечки информации — совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Выявление технических каналов утечки информации становится все более важным в нашем цифровом мире. Все данные, будь то личная информация, данные о корпоративной безопасности или государственные секреты, могут быть объектами утечки через различные каналы.

Основными объектами защиты информации являются информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.

Системы и средства, которые непосредственно обрабатывают такую информацию, называют основными техническими средствами и системами (ОТСС), однако в данном курсе наиболее (хорошее) определение техническими средствами приёма, обработки и хранения информации (ТСПИ).

Ход работы

1. Создайте документ электронной таблицы.

В Microsoft Excel, Google Таблицах или любой другой программе редактирования электронных таблиц создайте документ, в котором будет сформирован модуль для расчёта.

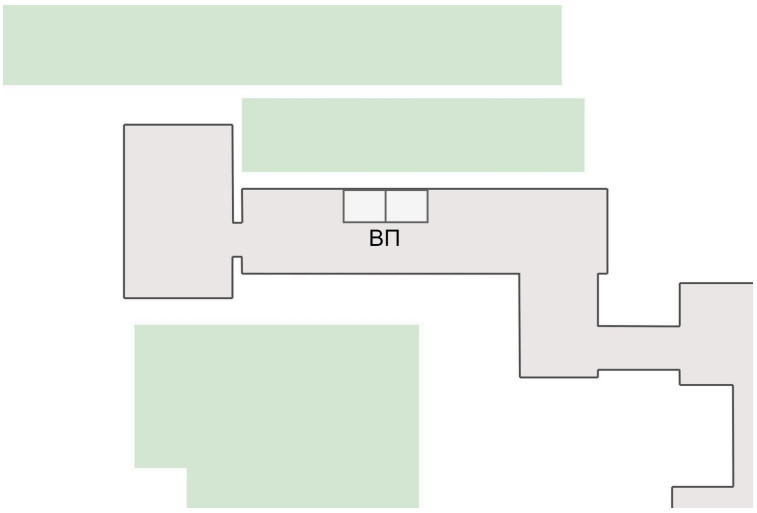
Создайте лист «Исходные данные». В него вы будете вносить все данные в этой работе.

2. Определите объекты защиты информации.

В здании вашего варианта стена к стене располагаются два выделенных помещения, которые вы будете анализировать. Придумайте им любое расположение и отметьте их на схеме. При этом расположение ВП должно соответствовать правилам:

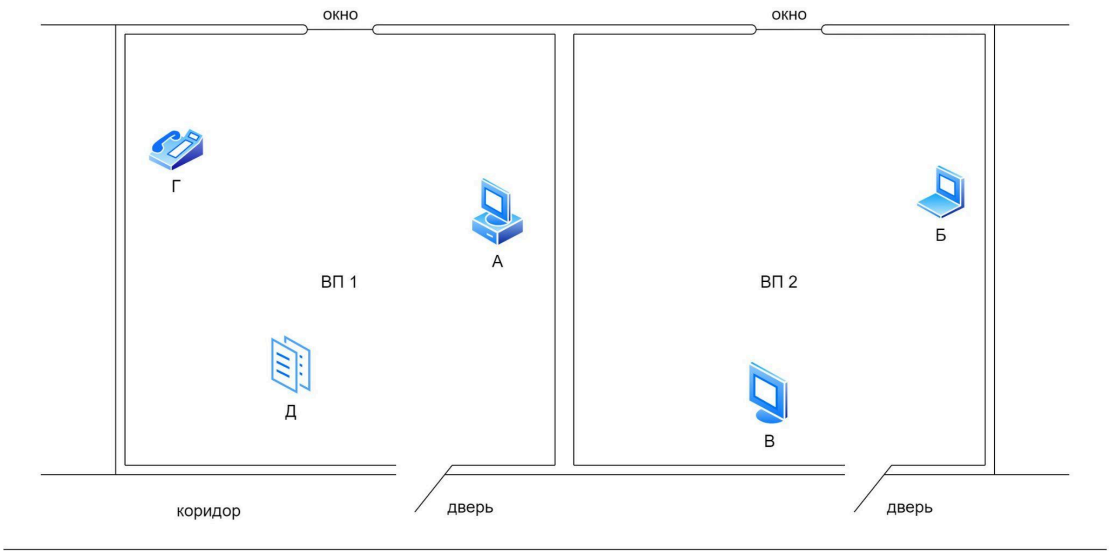
- Выделенное помещение должно находиться в основном здании (не в рядом стоящих отдельных постройках)
- Выделенное помещение должно находиться у стены здания (поскольку они имеют окна)
- Выделенные помещения располагаются рядом, поэтому на стене здания, с которой они граничат, должно быть как минимум два окна
- Окна выделенных помещений должны смотреть наружу контролируемой зоны, на улицу (применимо к зданиям сложной формы, где окна могут смотреть «внутрь» территории)

Поместите в отчёт схему с отмеченными выделенными помещениями. Ниже представлен пример размещения ВП на схеме:



Выделенным помещением называется помещение (кабинет, комната, аудитория), в которой ведётся работа с секретной, конфиденциальной информацией. Поскольку нарушитель знает, что в данном помещении находится секретная информация в том или ином виде, он захочет её получить, в связи с чем необходимо организовать защиту помещения от утечки информации по техническим каналам.

Схема выделенных помещений приведена на рисунке ниже.



На ней буквами обозначены пять объектов защиты информации.

- Буквой «А» отмечен персональный компьютер, на котором обрабатывается информация повышенной важности
- Буквой «Б» обозначено рабочее место рядового сотрудника организации
- Буквой «В» отмечен монитор общественного пользователя (например, экран отправления поездов, рекламный экран, проектор и т.п.)
- Буквой «Г» обозначен телефонный аппарат
- Буквой «Д» обозначены бумажные документы

Для каждого объекта придумайте его наименование исходя из его описания. Учтите, что объекты могут быть разными в зависимости от категории здания. Например, у государственной организации объектом «А» может быть компьютер с обрабатываемой на нём государственной тайной, а у школы — рабочее место бухгалтера.

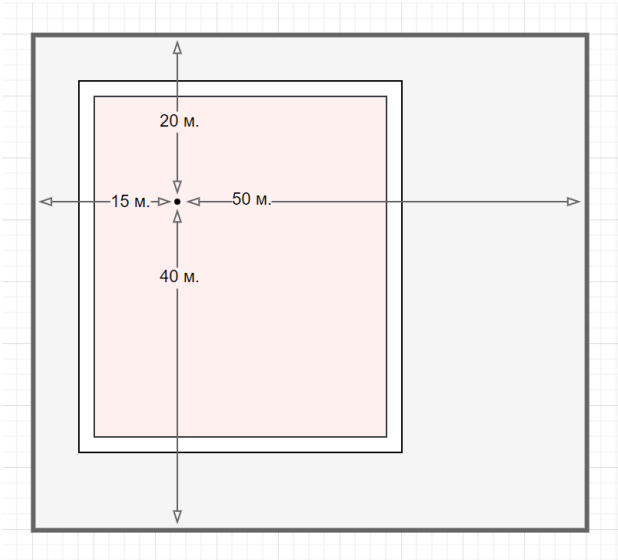
В отчёте укажите перечень объектов защиты в виде списка. В Excel составьте шаблон таблицы исходных данных, который может выглядеть примерно так:

Параметр	Объекты защиты				
	А	Б	В	Г	Д
(r) Расстояние до КЗ, м	...	...	...	...	...
...	...	...	...	...	...

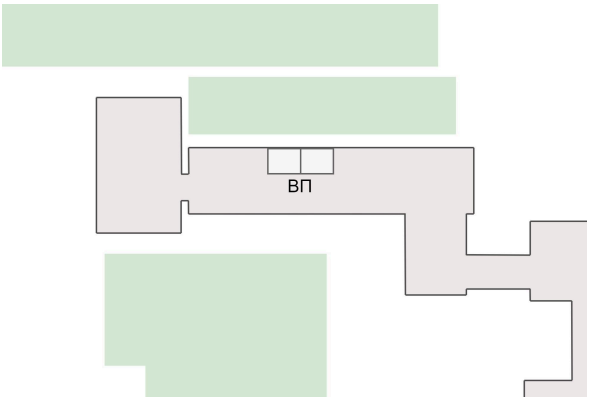
3. Определите расстояние до границы контролируемой зоны.

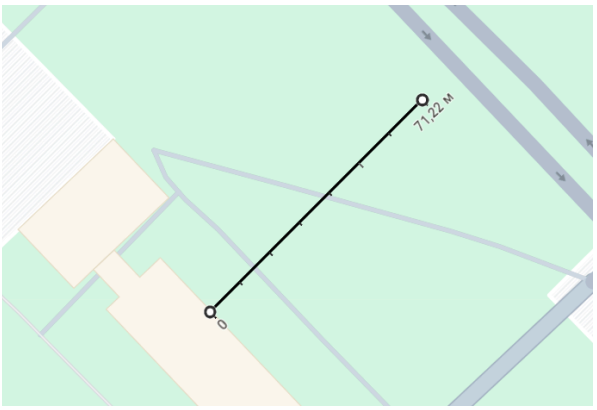
Внешний нарушитель, пытаясь перехватить конфиденциальную информацию, постарается быть как можно ближе к объекту защиты (компьютеру), однако пересечь границу контролируемой зоны он не может (в данной работе мы будем считать, что все заборы и стены неприступны для злоумышленника).

Таким образом, расстоянием от объекта защиты до границы контролируемой зоны называется минимальное среди всех таких расстояний. Например, на рисунке ниже расстояние от объекта защиты, помеченного точкой, до границы контролируемой зоны равняется 15 метрам.



Найдите минимальное расстояние от выделенных помещений до контролируемой зоны. Чтобы вычислить расстояния, используйте инструмент «Линейка» в картографических сервисах, ориентируясь на схему здания.





Внесите измеренные расстояния в таблицу. Поскольку размеры здания в несколько раз превосходят размеры помещения, положением объектов в помещении можно пренебречь, и расстояние до границы КЗ будет одинаковым для всех пяти объектов защиты.

4. Определите показатель затухания волн.

Показатель затухания волн — параметр, определяющий степень затухания электромагнитных волн с расстоянием. Волны затухают тем сильнее, чем больше преград встречается у них на пути. Обычно данный показатель находится в диапазоне от 1,3 (для открытых сельских районов) до 2,8 (для плотной городской застройки).

Для вашего варианта используйте формулу для вычисления этого показателя:

$$\text{Показатель затухания волн} = 1.7 + \frac{T + B + C - R}{15}$$

Где:

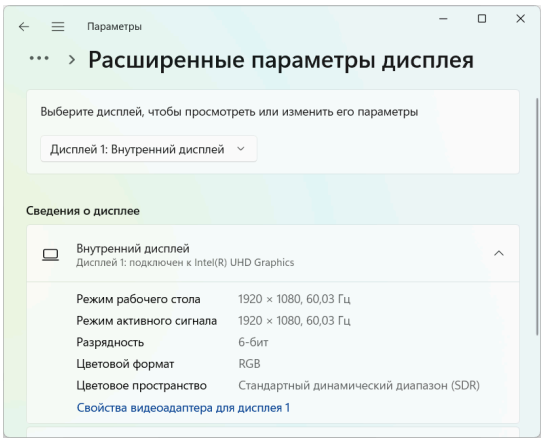
— *T* — коэффициент, отражающий наличие деревьев в окрестности здания (от 0 до 5, где 0 — нет деревьев, 5 — много деревьев)
— *B* — коэффициент, отражающий наличие посторонних зданий, преград и препятствий в окрестности здания (от 0 до 5, где 0 — нет преград, 5 — много преград)
— *C* — коэффициент, отражающий близость здания к другим зданиям (от 0 до 5, где 0 — здание находится в открытом пространстве, 5 — здание окружено другими зданиями)
— *R* — коэффициент, отражающий расположение здания относительно основных магистралей и дорог (от 0 до 5, где 0 — здание расположено рядом с основными дорогами, 5 — здание находится вдали от основных дорог)

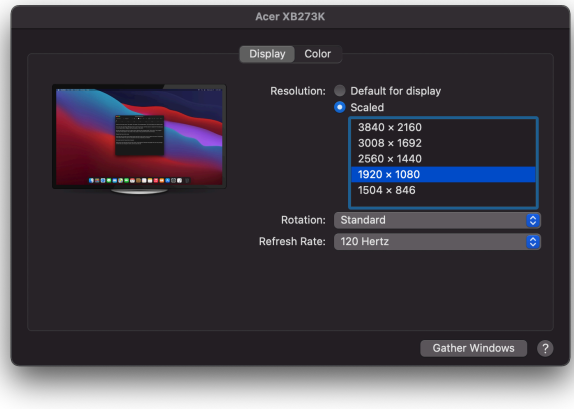
Внесите данный показатель в таблицу, он будет одинаковым для всех пяти объектов.

5. Измерьте показатели видеосистем компьютеров.

Наиболее опасным с точки зрения утечки информации режимом работы ПК является вывод информации на экран монитора. На мониторе отображаются текст, изображения, документы конфиденциального характера. Сам монитор излучает побочные электромагнитные излучения, которые могут распространяться за пределы контролируемой зоны, а значит, могут быть перехвачены нарушителем.

В качестве параметров для объекта «А» используйте параметры видеосистемы вашего компьютера или ноутбука. Их можно узнать в настройках дисплея.





В качестве параметров для объекта «Б» используйте параметры по варианту, которые указаны в практике № 0.

В качестве параметров для объекта «В» используйте стандартные параметры интерфейса VGA: разрешение экрана 640×480 пикселей, 16 цветов (4 бита), вертикальная частота обновления 60 Гц.

У объектов «Г» и «Д» нет мониторов, поэтому их поля можно оставить пустыми или заполнить нулями.

Внесите показатели видеосистемы (разрешение и частоту обновления экрана) в таблицу.

6. Определите виды информации и способы их представления.

Составьте таблицу, в которой содержатся данные об обрабатываемой или воспроизводимой информации на объектах защиты. Шаблон таблицы представлен ниже:

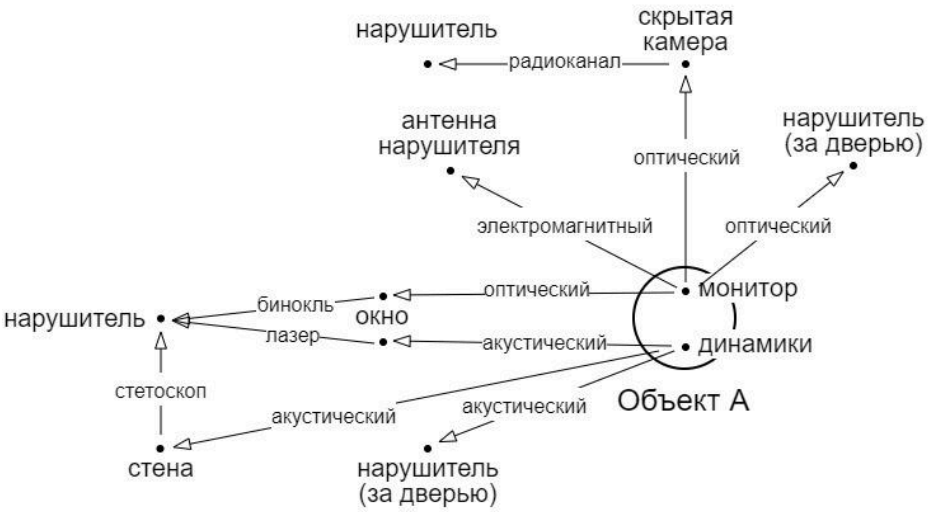
Объект защиты	**Информация**	**Способ представления**
А	Документы, представляющие коммерческую тайну	Отображение на экране
		Передача по каналу связи
		Хранение на жестком диске
	Документы, содержащие персональные данные	Отображение на экране
Б	...	...
	...	...

К объектам защиты добавьте также людей (сотрудников), ведущих конфиденциальные переговоры в помещении.

7. Составьте схему технических потоков информации.

В графическом редакторе составьте схему (граф) возможных потоков информации в выделенных помещениях. Предположите, какие могут быть приёмники информации (как в помещении, так и вне его) и обозначьте дугами-стрелками информационные потоки с указанием вида потока: оптический (видовой), акустический, электрический (по проводам), электромагнитный.

К примеру, часть вашей схемы (для одного объекта) может выглядеть так:



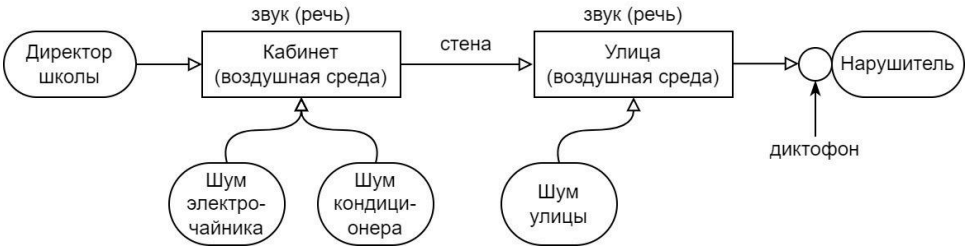
Объект «А» имеет монитор, отображающий информацию, и динамики, которые также могут проигрывать некоторую защищаемую информацию. Изображение с монитора нарушитель может подсматривать, стоя у приоткрытой двери или из окна соседнего здания (через бинокль), а также записывать на заранее установленную им скрытую камеру, которая передаёт информацию по радиоканалу. Кроме того, монитор излучает побочные электромагнитные излучения, которые нарушитель может перехватить антенной, стоя рядом со зданием. Информацию с динамиков нарушитель может подслушать, стоя у приоткрытой двери, прослушивая вибрации стены стетоскопом или направив на окно лазер, считывающий колебания стекла и преобразовывающий их в звук.

8. Постройте структурную и пространственную модели канала утечки.

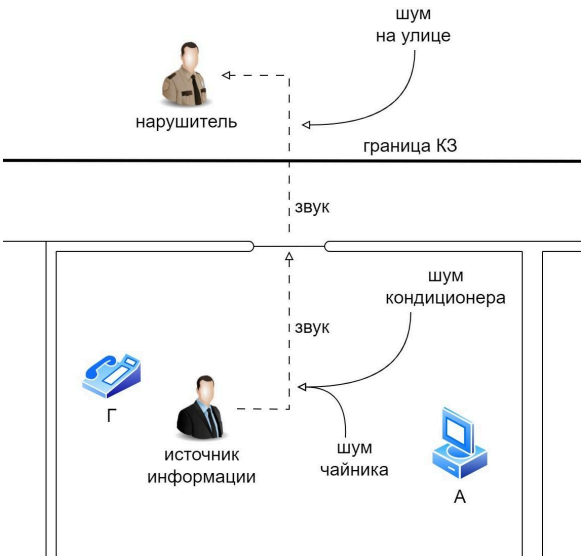
Из схемы, составленной вами в пункте 7, выберите любой канал утечки (любую строку таблицы) и опишите его, указав все основные элементы канала передачи информации: источник информации, источник сигнала, приёмник информации, приёмник сигнала, среда распространения, источник помех. Поскольку для одного канала возможны несколько приёмников, вам нужно выбрать один (на ваше усмотрение). Например, описание акустического канала утечки разговора директора школы может выглядеть так:

Рассмотрим акустический канал утечки информации от директора школы до нарушителя, стоящего у окна кабинета директора. Источником информации является директор школы, источник сигнала — речевой аппарат человека. Средой распространения звуковых волн является воздух. Приёмником сигнала является диктофон нарушите–ля, приёмником информации — нарушитель. Кроме того, в данном канале присутствуют помехи: шум электрических приборов в кабинете (электрочайник, кондиционер), шум на улице, а также стена здания, являющаяся причиной значительного затухания звуковых волн.

По данному описанию постройте структурную модель канала утечки. Структурная модель описывает структуру (состав и связи элементов) канала утечки. Например, для вышеприведённого описания структурная модель может выглядеть следующим образом:



Постройте пространственную модель канала утечки. Пространственная модель описывает расположение канала утечки информации, включая местоположение источника и приемника сигналов, расстояние от границы организации, направление распространения информации и ее протяженность. Графическое представление пространственной модели может быть выполнено в виде плана помещения, здания или территории организации, а также прилегающих участков среды.



Структурная и пространственная модели взаимно дополняют друг друга и не являются независимыми.

9. Оформите вывод по проделанной работе.

В выводе укажите, какие объекты выявлены в здании и через какие технические каналы утечки информации можно получить информацию.

Контрольные вопросы

Основные вопросы.

1. Что называют утечкой информации?
2. Что называют утечкой информации по техническому каналу?
3. Что такое технический канал утечки информации?
4. Опишите схему технического канала утечки информации
5. Что такое технические средства передачи, обработки, информации ограниченного доступа?
6. Опишите состав ТСПИ
7. Перечислите основные технические каналы утечки информации
8. Как делятся технические каналы утечки информации по времени функционирования?
9. Какие виды угроз существуют при использовании технических каналов?
10. Каковы основные причины утечки информации через технические каналы?

Бонусные вопросы.

1. В чём отличие потенциальных и реальных технических каналов утечки информации?
2. Что такое активный и пассивный каналы утечки информации?
3. Как шифрование может помочь в предотвращении утечек информации?
4. Какие физические методы защиты от утечки информации через технические каналы существуют?
5. Какие законы и нормативные акты регулируют область технических каналов утечки информации?
6. Каковы последствия утечки информации через технические каналы?
7. Что такое составной канал утечки информации? Приведите примеры