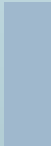


Технические средства защиты информации



Технические каналы утечки информации

- Под **техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают **способ получения с помощью ТСР разведывательной информация** об объекте. Причем под **разведывательной информацией** обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Состав объекта ТСПИ

- технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа, вместе с их соединительными линиями;
- вспомогательные технические средства и системы вместе с их соединительными линиями;
- посторонние проводники;
- система электропитания объекта;
- система заземления объекта.

Способы перехвата информации обрабатываемой техническими средствами



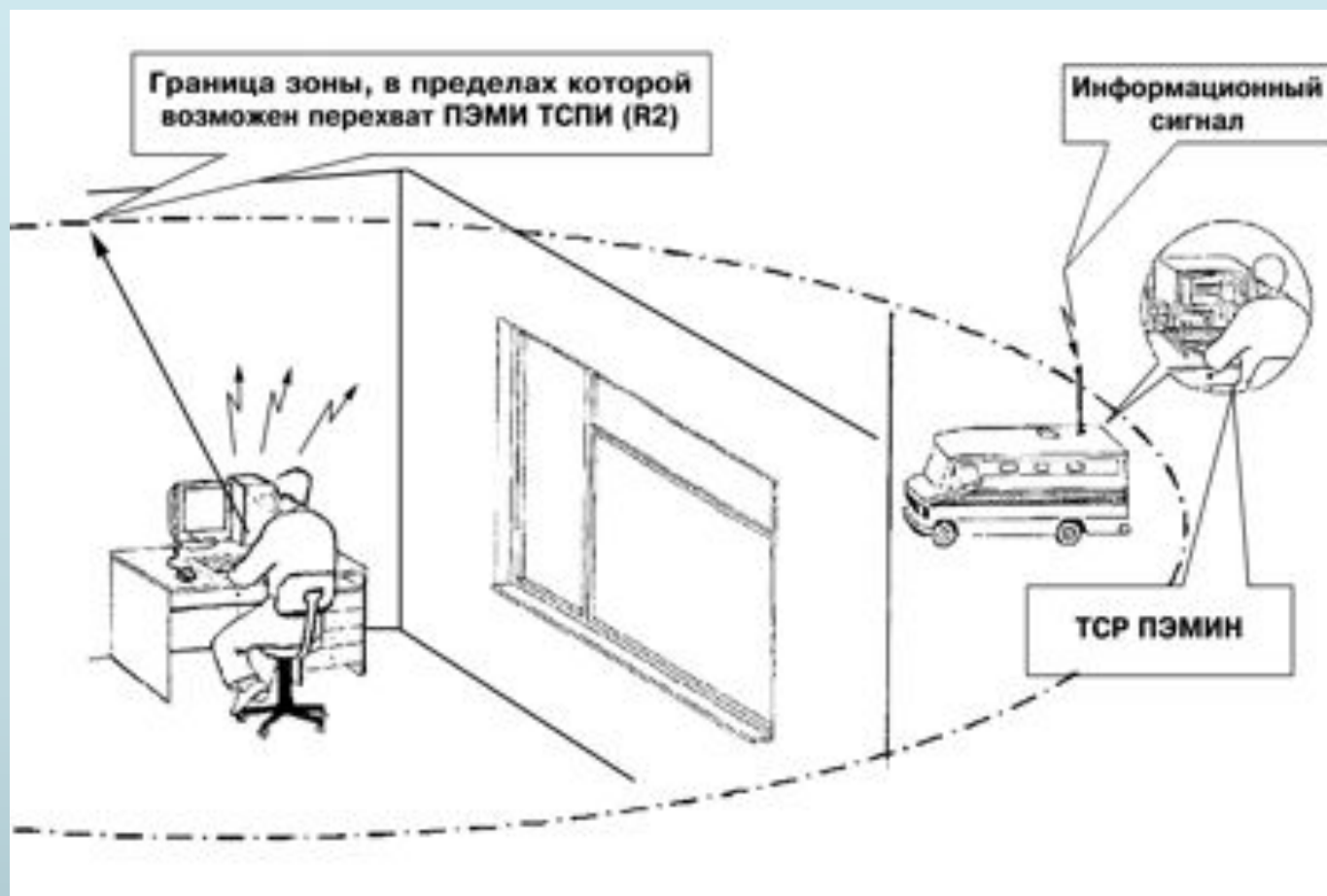
Перехват побочных электромагнитных излучений

- побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;
- побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;
- побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения

- В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Побочные электромагнитные излучения



Побочные электромагнитные излучения на частотах работы высокочастотных генераторов

- В состав ТСПИ могут входить различного рода высокочастотные генераторы
- В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы.

Пример

Работающее электрооборудование (например, дисплеи, накопители и т. п.) несанкционированно излучает в эфир информацию.

Дисплей (ЭЛТ), состоит из устройств горизонтальной развёртки, вертикальной развёртки, видео усилителя, блоков питания и устройства вывода визуальной информации.

Мощные каналы видео усилителя и отходящие от них соединительные проводники можно рассматривать как передатчик, несанкционированно излучающий информацию. Информация может быть восстановлена с помощью обычного телевизора, но без сигналов синхронизации.

Маркус Кун

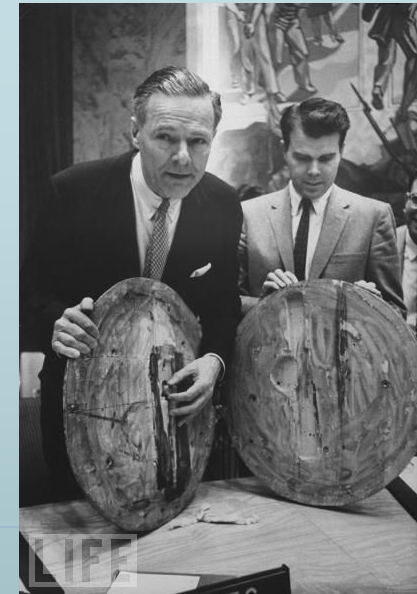
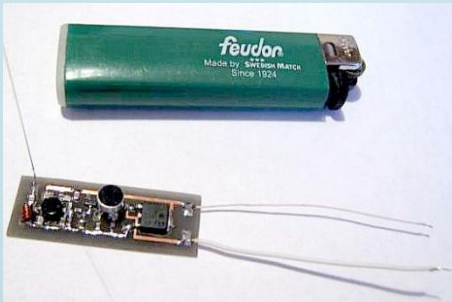
- Доктор из Кембриджского Университета продемонстрировал, возможно через две комнаты и три стены перехватить изображения на ЖК-экране. С оборудованием стоимостью около 1000 фунтов стерлингов. Ранее считалось, что ЖК-мониторы не имеют вышеупомянутой уязвимости.
- Он же предложил способ оптического съёма информации с ЭЛТ мониторов. Информация восстанавливается из рассеянного света (например света отражаемого лицом оператора)

Средства акустической разведки

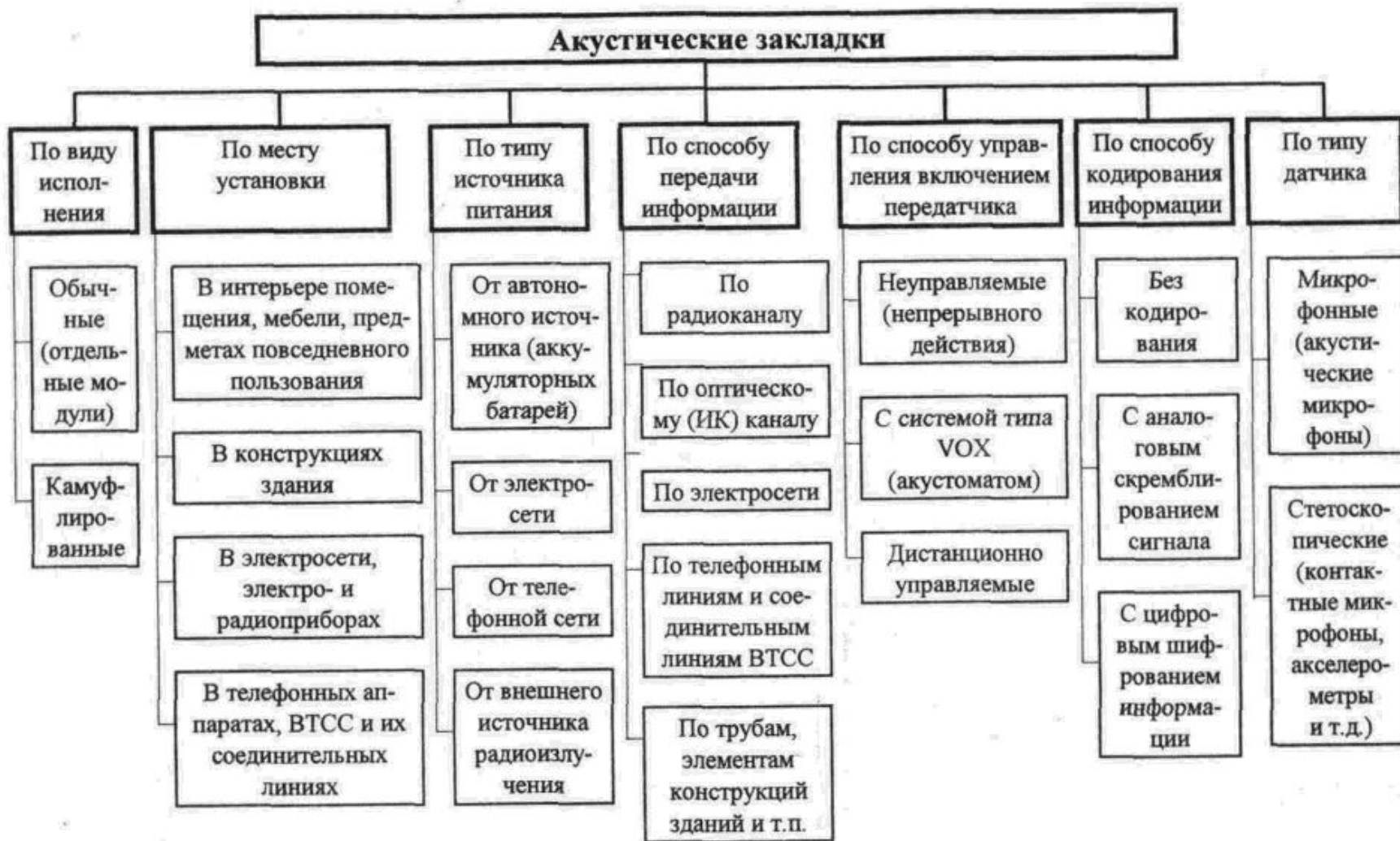
- В основе всех средств акустической разведки лежит использование микрофонов. Микрофоны - это преобразователи акустических колебаний в электрические (за исключением ряда особых случаев).
- Существуют классификации микрофонов по:
 - принципу электромеханического преобразования
 - акустическим характеристикам

Радио закладки

- В общем случае, устройство работающее как радиопередатчик.



Классификация акустических закладок



Простые в обнаружении радио закладки

□ Передатчики непрерывного действия

- Они постоянно излучают в эфир радиосигналы, соответственно любое оборудование, которое предназначено для поиска источников излучения позволит обнаружить устройство при первой проверке
- При использовании автономного источника питания, требуют частой замены элементов питания, которая повышает вероятность демаскировки устройства.

Проще всего: разместить, достать, использовать.

Низкая стоимость.



Средняя сложность обнаружения

- Дистанционно управляемые или VOX устройства.
 - Большую часть времени практически не излучают ничего в эфир
 - Меньшие затраты энергии

Более сложны в эксплуатации, большие габариты, требуют большей продуманности действий при использовании.



Трудно обнаружимые

- Цифровые диктофоны, с передачей данных по команде оператора.

- Большую часть времени ничего не излучают в эфир

- Ввиду отсутствия двигателей и устройств подмагничивания, не создают магнитного поля(в сравнении с плёночными устройствами)

- Передают запись, по запросу оператора.

Одним из единственных недостатков является получение информации с задержкой, что чаще всего допустимая жертва.



Трудно обнаружимые радио закладки

- Пассивные микрофоны, т.н. эндовибраторы
 - По сути устройства с отсутствующим элементом питания, в классификации – «от внешнего источника радиоизлучения»
 - Практически не обнаружимы при правильном использовании
 - Не требуют замены источника питания ввиду его отсутствия
 - Включаются при интенсивном радио облучении
 - Не обнаружимы нелинейными локаторами

Термен

Радиостетоскопы

- Могут быть установлены вне контролируемого помещения
- Трудно обнаружимы
- Легко устанавливаются и обслуживаются, в случае свободного доступа в здание

Радио закладки

- Любое устройство рассматриваемого типа, принадлежит к одному(и только к одному) пункту из классификации. Каждый из них обеспечивает большую или меньшую вероятность раскрытия.
- Обычно меньшая вероятность раскрытия идёт в ущерб дальности передачи, длительности работы, «удобству» использования и пр.

Защита от радио закладок

- Ограничение доступа в помещение
- Экранирование помещения(«клетка Фарадея»)
- Использование широкополосных генераторов помех

Ограничение доступа в помещение

- Доступ в помещение осуществляется только по специальной санкции
- Посещение помещения контролируется службой безопасности
- Количество предметов в помещении ограничено
- Используется минимум коммуникаций

Экранирование помещения(«клетка Фарадея»)

- Помещение экранируется для ограничения распространения радио сигналов.
- Все выходящие коммуникации подвергаются зашумлению



Инфракрасные акустические закладки

- Для передачи сигнала используется оптический канал, данные передаются в невидимом глазу ИК диапазоне
- Дальность передачи может составлять до нескольких сот метров
- Обнаруживается только приёмниками оптического излучения и нелинейными локаторами

Акустические закладки с проводной передачей

- Тяжело обнаружить
- Обычно не требуют автономного источника питания
- Могут передавать информацию на значительные расстояния

- Трудны в установке
- Чаще всего требуют постоянного доступа в здание, т.к. по мере удаления от устройства передаваемый сигнал затухает

Алгоритмические средства защиты

- Скремблирование- обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности.
- Блочное шифрование



Микрофонный эффект

- Название явления при котором некоторая часть электрической цепи воспринимает звуковые колебания и вибрацию подобно микрофону.
- Характерен для старых телефонных аппаратов, систем звукового оповещения и множества других приборов.

Защита от микрофонного эффекта

- Выключение из сети приборов обладающих микрофонным эффектом
- Установка дополнительного оборудования для фильтрации сигналов в цепи
- Для осуществления любых защитных мер необходимо определить устройства обладающие микрофонным эффектом.

Аппаратные кейлоггеры

- Устройство позволяет перехватывать сигнал с клавиатуры компьютера
- Обычно включается в разрыв между системным блоком и клавиатурой, соответственно не обнаружимо из системы
- В зависимости от реализации может передавать данные по беспроводной сети



Нелинейный локатор

- Может обнаруживать и определять местоположение любых электронных устройств, независимо от того, работают они или нет



Химические ловушки



Заключение

- Защита от утечки информации по техническим каналам обеспечивается в первую очередь политикой безопасности
- Практически невозможно обеспечить защиту от утечки в арендуемых помещениях, планы постройки которых не известны или при аренде отдельных офисов

Задания

- Рассказать о ВЧ навязывании и методах защиты от него
- Рассказать о работе Ван Эйка (Wim van Eck) по перехвату изображений с мониторов
- Рассказать о работах Маркуса Куна (Markus G. Kuhn) на тему перехвата изображений с ЖК экранов

Задания

□ Знать:

- Определения ТСПИ и ТКУИ
- Способы перехвата информации передаваемой ТСПИ
- Достоинства и недостатки акустических закладок, в зависимости от их принадлежности к определённому классу
- Методы выявления акустических закладок, если они существуют