Технические методы и средства защиты информации

ВВЕДЕНИЕ

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

- **Инженерно-техническая защита информации** - предотвращение утечки информации по различным техническим каналам
- **Основные объекты защиты информации**
- 1). Информационные ресурсы, содержащие сведения, связанные с конфиденциальной информацией и государственной тайной.
- 2). Технические средства приёма, обработки и хранения информации (ТСПИ):

Основные объекты защиты информации

Технические средства приёма, обработки и хранения информации (ТСПИ):

- Средства и информационные системы (средства вычислительной техники, сети и системы),
- программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение),
- системы связи и передачи данных,
- технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства),
- средства изготовления, тиражирование документов
- другие технические средства обработки графической и буквенно-цифровой информации, обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны.

Вспомогательные технические средства и системы (ВТСС). Технические средства и системы, не входящие в состав ТСПИ, но расположенные в помещениях обработки конфиденциальной информации:

- системы пожарной и охранной сигнализации,
- технические средства телефонной, громкоговорящей связи, радиотрансляции,
- контрольно-измерительная аппаратура,
- электробытовые приборы,
- помещения, предназначенные для обработки данной информации имеющей ограниченное распространение.

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, могут проходить провода и кабели, не относящиеся к ТСОИ и ВТСС, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, которые называются **посторонними проводниками**

Электропитание ТСОИ и ВТСС осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной подстанцией городской электросети.

Технические каналы утечки информации

Наибольшую возможность образования каналов утечки информации представляют ТСПИ и ВТСС, имеющие непосредственный выход за пределы контролируемой зоны (КЗ).

Контролируемая зона - это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа

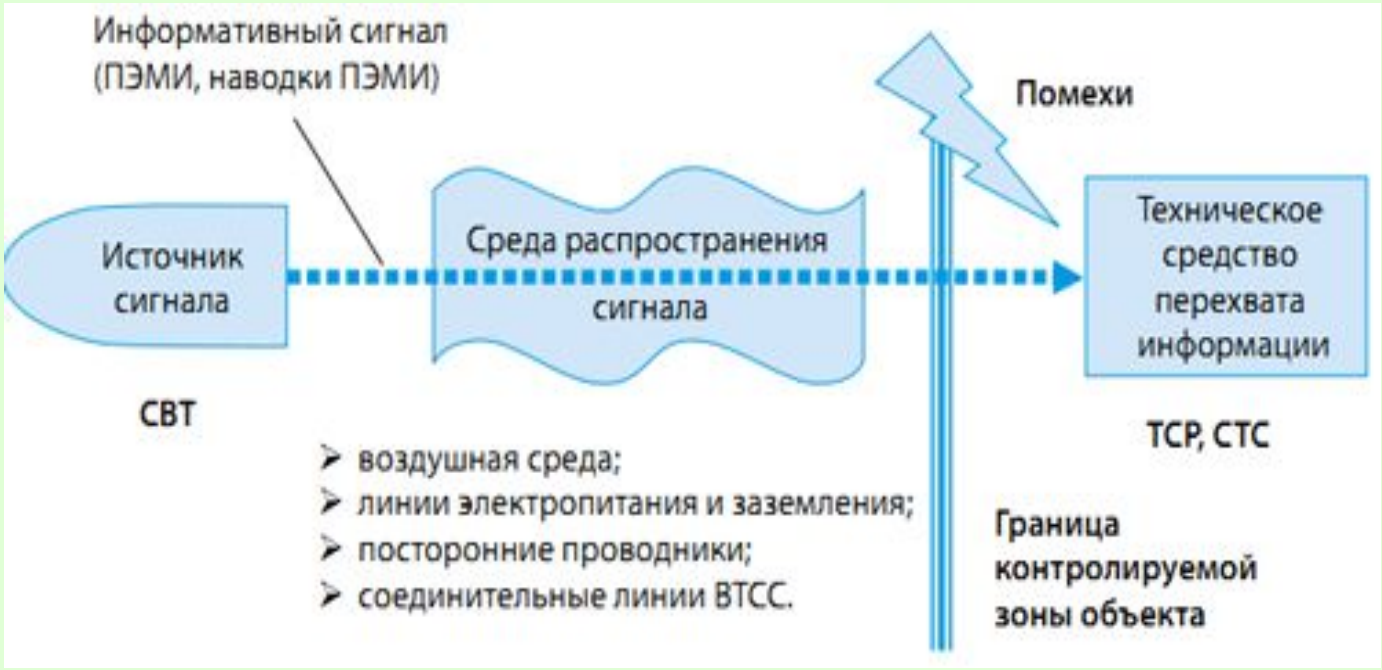
Контролируемая зона может ограничиваться периметром охраняемой территории, либо большим размером, чем охраняемая территория, но при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории

- Зона с возможностью захвата разведывательным оборудованием сигналов, содержащих секретную информацию, называется опасной зоной

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

Технический канал утечки информации (ТКУИ) совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется данный информационный сигнал, т.е. под ТКУИ подразумевают способ получения с помощью ТСР любой разведывательной информации об объекте.

В зависимости от природы возникновения, сигналы распространяются в различных физических средах.



Средой распространения могут являться твердые, газовые (воздушные) и жидкостные (водные) среды.

Электромагнитные волны распространяются в любой среде (даже в вакууме).

К средам распространения относят воздушное пространство, соединительные линии и токопроводящие элементы, конструкции зданий, грунт и другие.

Источник сигнала :

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник акустических волн, модулированных информацией.

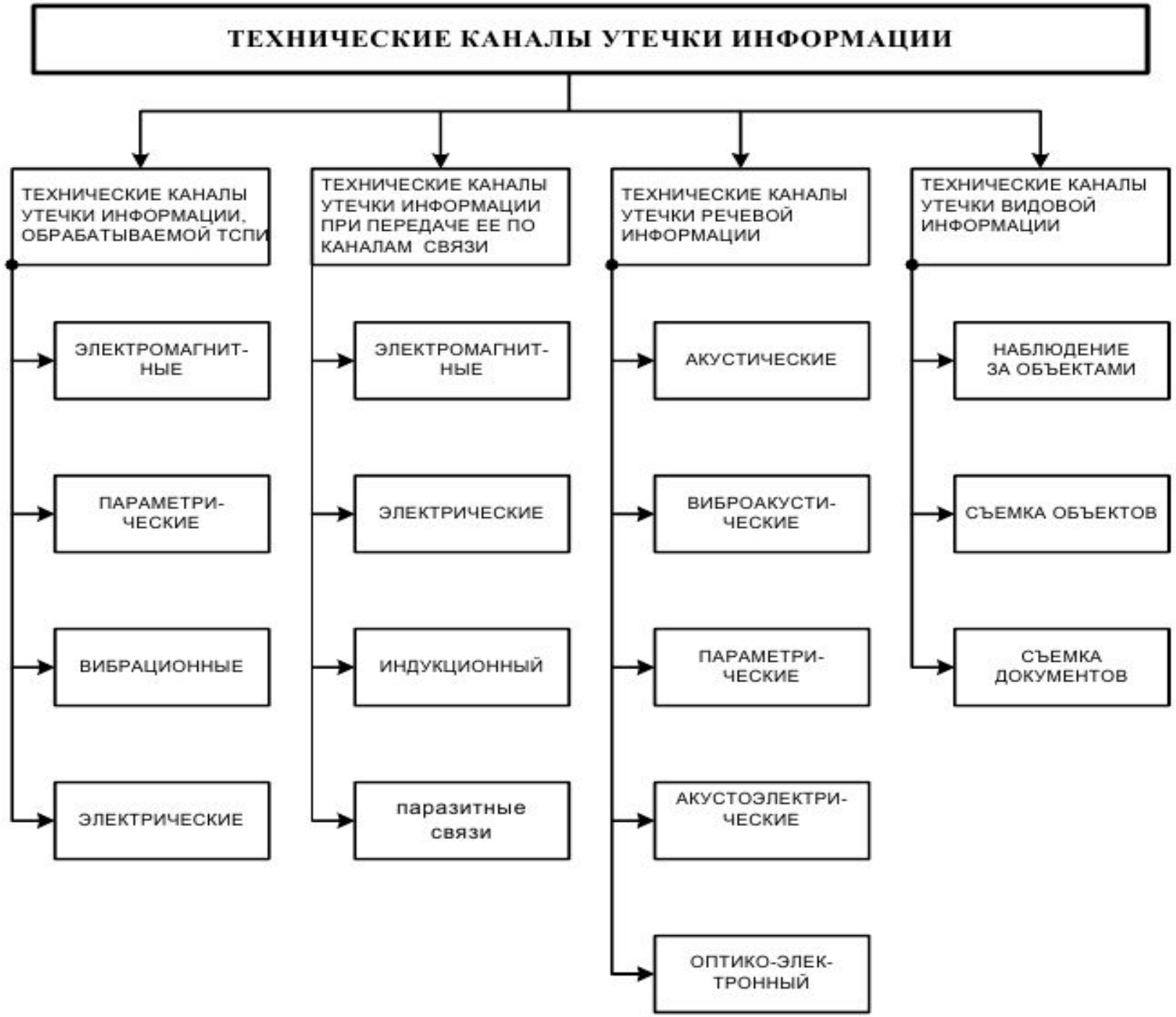
Параметры среды распространения сигнала :

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Функции приемника:
выбор носителя с нужной получателю информацией;
усиление принятого сигнала до значений,
обеспечивающих съем информации;
съем информации с носителя;
преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

описание ТКУИ должно включать в себя:
источник угрозы (приемник информативного сигнала)
среда передачи информационного сигнала
источник (носитель) информации


ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТСПИ
ЭЛЕКТРОМАГНИТ-НЫЕ
ПАРАМЕТРИ-ЧЕСКИЕ
ВИБРАЦИОННЫЕ
ЭЛЕКТРИЧЕСКИЕ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ЕЕ ПО КАНАЛАМ СВЯЗИ
ЭЛЕКТРОМАГНИТ-НЫЕ
ЭЛЕКТРИЧЕСКИЕ
ИНДУКЦИОННЫЙ
паразитные связи
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ
АКУСТИЧЕСКИЕ
ВИБРОАКУСТИ-ЧЕСКИЕ
ПАРАМЕТРИ-ЧЕСКИЕ
АКУСТОЭЛЕКТРИ-ЧЕСКИЕ
ОПТИКО-ЭЛЕК-ТРОННЫЙ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ
НАБЛЮДЕНИЕ ЗА ОБЪЕКТАМИ
СЪЕМКА ОБЪЕКТОВ
СЪЕМКА ДОКУМЕНТОВ

Классификация каналов утечки информации обрабатываемой ТСПИ

I. Электромагнитные:

- электромагнитные излучения элементов ТСПИ;

При протекании тока по элементам ТСПИ и соединительным линиям возникает переменное электрическое и магнитное поле, модулированное по закону изменения информационного сигнала.

- электромагнитные излучения на частотах ВЧ-генераторов ТСПИ;

В состав ТСПИ могут входить высокочастотные генераторы (задающие, тактовой частоты, измерительных приборов и т.д.). В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах генераторов наводятся электрические сигналы, вызывающую непреднамеренную модуляцию колебаний генераторов, которые излучаются в окружающее пространство.

- излучения на частотах самовозбуждения усилителей низкой частоты.

- в элементах ТСПИ (например, усилителях систем звукоусиления и, магнитофонов, систем громкоговорящей связи и т.п.), возможен перевод усилителя из режима усиления в режим автогенерации сигналов за за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители на магнитных носителях;
- чтение информации с накопителей на магнитных носителях;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства – принтеры, плоттеры;-
запись данных от сканера на магнитный носитель (ОЗУ).

Основными источниками возникновения ПЭМИ при работе СВТ являются:

- Процессор, шина данных процессора и цепи питания.
- Контроллеры и мост чипсета.
- Модули памяти и шина данных.
- Инверторы питания перечисленных выше устройств.
- HDD и шины IDE (ATA) и SATA.
- CD и шина IDE (ATA).
- Видеокарта и шина AGP или E-PCI.
- COM порт и внешние подключения по нему.
- LTP порт и внешние подключения по нему.
- USB порт.
- VGA и другие виды портов, предназначенные для подключения мониторов.
- Беспроводные сетевые адаптеры IEEE 802 для локальных сетей.

ПРИМЕР

Для примера возьмем монитор ПЭВМ. Первичным генератором сигналов является видеокарта, находящаяся в системном блоке ПЭВМ. В видеокарте находятся три ЦАП (для каждого луча R,G и B) которые передают импульсные сигналы амплитудой около 3 В по кабелю к монитору. Далее, в мониторе эти сигналы усиливаются усилителями токов лучей до нескольких десятков вольт и подаются на электронно-лучевую трубку.

Какие антенные системы имеются у связки ПЭВМ – монитор?

Первая антенная система это кабель, соединяющий видеокарту с монитором, длина которого составляет около 1.5м. Вторая антенная система – отрезки проводников идущих от усилителей токов лучей к ЭЛТ, длина которых составляет 15 - 25 см.

Анализируя эти две антенные системы, можно сделать вывод, что они обе принимают участие в процессе излучения сигнала и основной вклад в излучение низкочастотных сигналов следует ожидать от кабеля видеоадаптера, а вклад в излучение сигналов высших гармоник можно ожидать от видеомонитора.

Данное разделение весьма условно и зависит от конструкции конкретного экземпляра ПЭВМ, качества сборки и расположения его узлов и кабелей.

Клавиатура

Стандартная клавиатура обычно имеет очень высокий уровень излучения. В тоже время с клавиатуры вводятся очень критичные с точки зрения безопасности данные, включая пароли пользователей и администратора системы. Излучение клавиатуры относительно узкополосное и сосредоточено, в основном, в области коротких и ультракоротких волн. Для его перехвата может использоваться очень дешевый коротковолновый разведывательный приемник. Учитывая также, что данные, вводимые с клавиатуры, вводятся в последовательном коде и поэтому могут быть легко интерпретированы, излучения, создаваемые клавиатурой, следует считать наиболее опасными.

Информация принтеров, клавиатуры передаётся последовательным кодом, все параметры этого кода стандартизированы и хорошо известны.

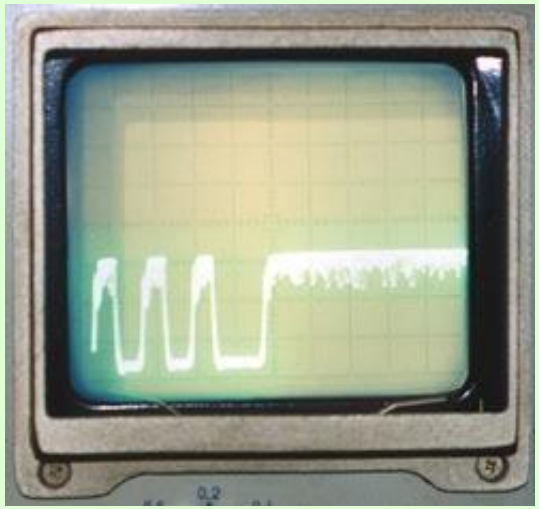


Рис. 1. Последовательный код знака = на экране осциллографа, подключенного к коротковолновому приемнику

Потенциально-информативные ПЭМИ

Совокупность составляющих спектра ПЭМИ, порождаемая протеканием токов в цепях, по которым передаются содержащие конфиденциальную (секретную, коммерческую и т. д.) информацию сигналы, называются **потенциально-информативными излучениями (потенциально-информативными ПЭМИ).**

Для персонального компьютера потенциально-информативными ПЭМИ являются излучения, формируемые следующими цепями:

- цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате;
- цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора;
- цепи, формирующие шину данных системной шины компьютера;
- цепи, формирующие шину данных внутри микропроцессора, и т. д.

Неинформативные ПЭМИ

Практически в каждом цифровом устройстве существуют цепи, выполняющие вспомогательные функции, по которым никогда не будут передаваться сигналы, содержащие закрытую информацию. Излучения, порождаемые протеканием токов в таких цепях, являются безопасными в смысле утечки информации. Для таких излучений вполне подходит термин **«неинформативные излучения (неинформативные ПЭМИ)»**. С точки зрения защиты информации неинформативные излучения могут сыграть положительную роль, выступая в случае совпадения диапазона частот в виде помехи приему информативных ПЭМИ (в литературе встречается термин «взаимная помеха»).

Для персонального компьютера неинформативными ПЭМИ являются излучения, формируемые следующими цепями:

- цепи формирования и передачи сигналов синхронизации;
- цепи, формирующие шину управления и шину адреса системной шины;
- цепи, передающие сигналы аппаратных прерываний;
- внутренние цепи блока питания компьютера и т. д.

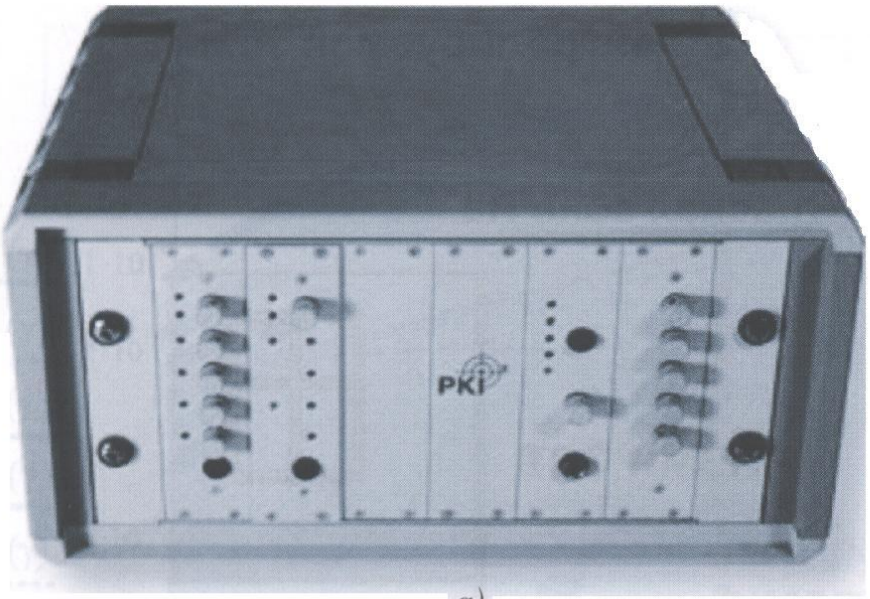
Безопасные информативные ПЭМИ

На практике могут встретиться ситуации, когда восстановление информации при перехвате потенциально информативных излучений какой-либо электрической цепи (цепей) невозможно по причинам принципиального характера.

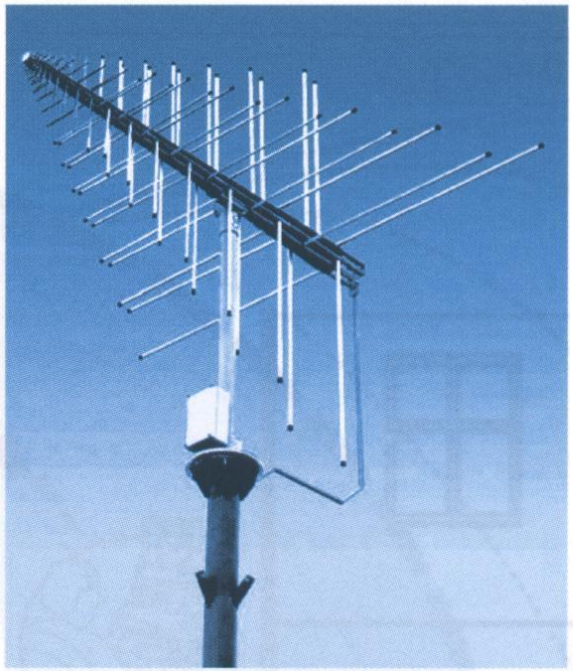
Например:
применение многоразрядного параллельного кода (для передачи каждого разряда используется своя электрическая цепь) в большинстве случаев (в зависимости от разрядности кода, формата представления информации) делает невозможным восстановление информации при перехвате ПЭМИ.
Потенциально информативные ПЭМИ, выделение полезной информации из которых невозможно при любом уровне этих излучений, называются **безопасными информативными излучениями (безопасными информативными ПЭМИ)**.

К безопасным информативным излучениям ПК можно отнести излучения цепей, формирующих шину данных системной шины и внутреннюю шину данных микропроцессора, а также излучения других цепей, служащих для передач информации, представленной в виде многоразрядного параллельного кода.

Образцы оборудования для перехвата ПЭМИ.



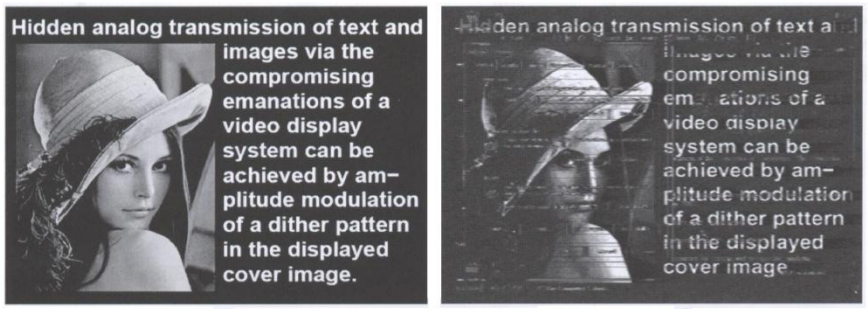
а)



б)

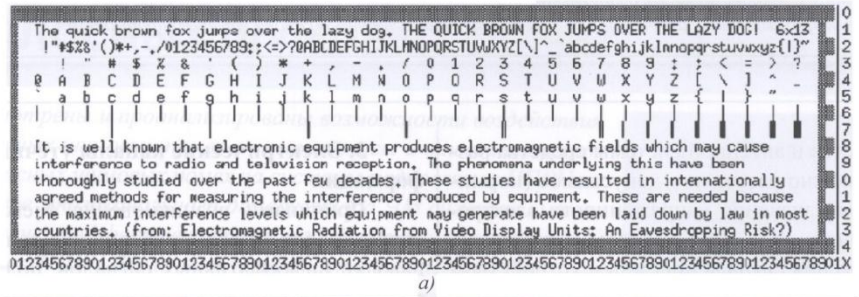
Комплекс перехвата побочных электромагнитных излучений СВТ:
а) специальное приёмное устройство PKI 2715 (дальность перехвата ПЭМИ от 10 до 50 м);
б) широкополосная направленная антенна R&S HL 007 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ)

Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.



а) *б)*

Тестовое изображение, выведенное на экран монитора (а) и изображение, перехваченное средством разведки ПЭМИ (б)



а)

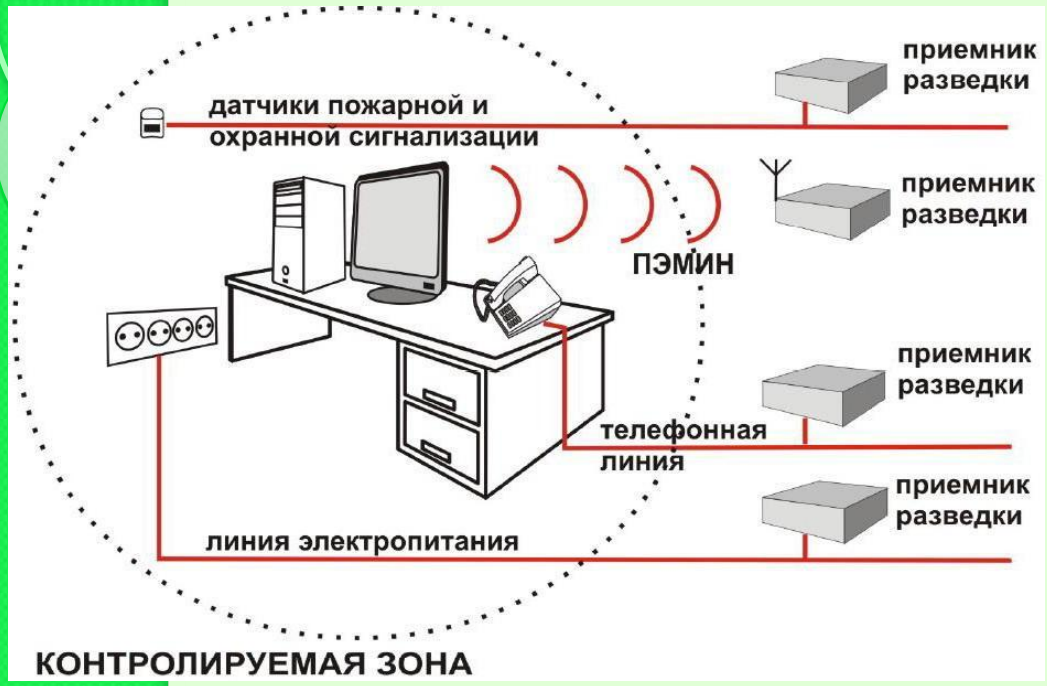
б)

Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800×600 @ 75Hz, тактовая частота $F_т$ = 49,5 МГц, размер букв 6×13 пикселей) (а) и текст, перехваченный средством разведки ПЭМИ ($\Delta F_{пр}$ = 200 МГц) (б)

II. Электрические:

- наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
- просачивание информационных сигналов в линии электропитания;
- просачивание информационных сигналов в цепи заземления;
- съем информации с использованием закладных устройств.

Понятие ПЭМИН.



Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей.

Электромагнитные наводки могут приводить к утечке информации по токопроводящим коммуникациям, имеющим выход за пределы контролируемой зоны.

Причинами возникновения электрических каналов утечки информации являются наводки информативных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

- наводки информативных сигналов в электрических цепях ТСОИ;
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках;
- наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями (“просачивание” информативных сигналов в цепи электропитания через блоки питания ТСОИ);
- наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

III. Параметрические:

- перехват информации путем «высокочастотного облучения» ТСПИ;

IV. Вибрационные:

- соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

I. Электромагнитные:

- электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

II. Электрические:

- подключение к линиям связи.

III. Индукционный канал:

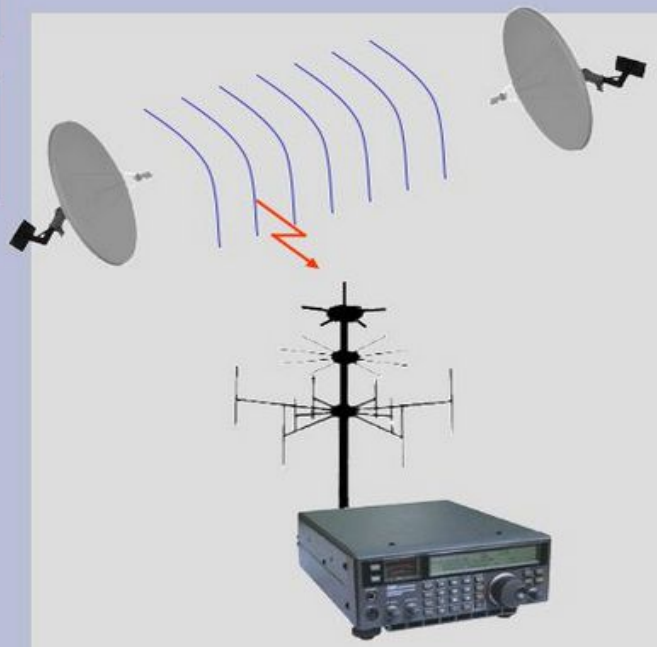
- эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

IV. Паразитные связи:

- паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

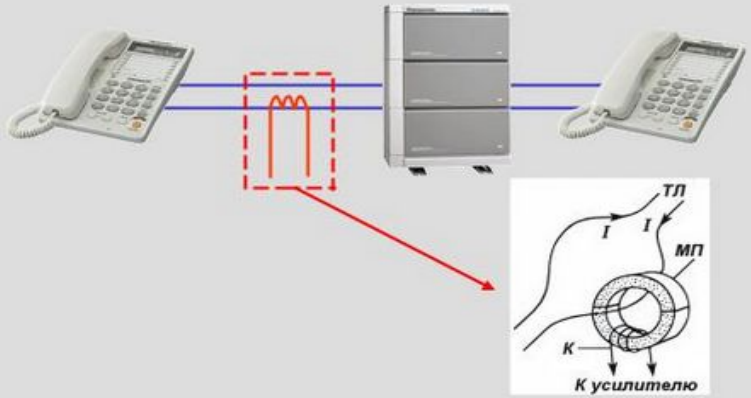
КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПРИ ЕЁ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

Электромагнитный



Электрический

Индукционный



ТЕХНИЧЕСКИЕ КАНАЛЫ перехвата информации передаваемой по каналам связи

- **Электромагнитый ТКУИ** - перехват электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию
- **Электрический ТКУИ** - съем информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Может использовать параллельное или последовательное подключение к линии связи.
- **Индукционный ТКУИ** - бесконтактный съем информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника..Бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи.

Технические каналы утечки речевой информации

I. Акустические каналы:

- среда распространения - воздух.

II. Виброакустические каналы:

- среда распространения - ограждающие строительные конструкции.

III. Параметрические каналы:

- результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала в информационный.

IV. Акустоэлектрические каналы:

- преобразование акустических сигналов в электрические

V. Оптико-электронный канал (лазерный):

- облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

I. Наблюдение за объектами:

- для наблюдения днем применяются оптические приборы и телевизионные камеры;
- для наблюдения ночью - приборы ночного видения, телевизионные камеры, тепловизоры.

II. Съемка объектов:

- для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи

III. Съемка документов:

- Съемка документов осуществляется с использованием портативных фотоаппаратов.

Перечисленные пути несанкционированного доступа по техническим каналам требуют достаточно профессиональных технических знаний и соответствующих программных или аппаратных разработок со стороны взломщика.

Однако злоумышленники не пренебрегают и другими способами добычи нужной информации, такими как:

- инициативное сотрудничество;
- склонение к сотрудничеству со стороны взломщика;
- хищение носителей информации и документальных отходов;
- подслушивание;
- выпытывание,
- и другие.


Специально создаваемые ТКУИ, обрабатываемой СВТ.
Активные способы перехвата информации, обрабатываемой СВТ.
Высокочастотное облучение СВТ.
Установка в СВТ специальных закладных устройств.
Использование технологии Soft Tempest

Принцип перехвата информации, обрабатываемой СВТ, методом “высокочастотного облучения”.

Перехват информации, обрабатываемой СВТ, методом «высокочастотного облучения»

В зависимости от схемы и способа использования энергии спецсредства негласного получения информации делятся на:

1) пассивные (переизлучающие)

и

2) активные (излучающие).

Активные спецсредства

Обязательными элементами всех активных спецсредств является **датчик** или **сенсор контролируемой информации**, преобразующий информацию в электрический сигнал.

Усилитель-преобразователь, который усиливает сигнал и преобразует его в ту или иную форму для последующей передачи информации.

Форма сигнала может быть аналоговой или цифровой. Обязательным элементом активных спецсредств съема информации является **оконечный излучающий модуль**.

Пассивные устройства

- не излучают вовне дополнительную энергию.

Для получения информации от подобных устройств с удаленного контрольного пункта в направлении контролируемого объекта направляется мощный сигнал.

Достигая объекта, сигнал отражается от него и окружающих предметов и частично возвращается на контрольный пункт.

Отраженный сигнал несет в себе информацию о свойствах объекта контроля.

К пассивным спецсредствам формально можно отнести практически все средства перехвата информации на естественных или искусственных каналах связи.

Все они энергетически и физически скрытны.

Самым распространенным и относительно недорогим способом негласного съема информации до сих пор остается установка разнообразных закладок (жучков).

Закладное устройство – скрытно устанавливаемое техническое средство негласного съема информации.

Одни из них предназначены для получения акустической информации, другие – для получения видовых изображений, цифровых или аналоговых данных от вычислительных средств и средств оргтехники, средств связи, телекоммуникации и др.

Существует огромное количество подобных устройств.

Они различаются исполнением и способом передачи информации – автономные или сетевые.

Могут быть изготовлены в виде:

- стандартных элементов существующих силовых и слаботочных линий (вилок, разъемов и т. п.),
- авторучек,
- пепельниц,
- картона,
- «забытых» личных вещей,
- стандартных элементов телефонных аппаратов и т. п.

К этой же категории средств относятся различные варианты миниатюрных диктофонов, микрокамер, телекамер и проч.

Более дорогие и предназначенные для продолжительного контроля технические средства заранее устанавливаются на объектах контроля (например, в период капитального или косметического ремонта).

Это могут быть проводные средства с микрофонами, глубоко замаскированные закладки (например, в вычислительной технике), средства акустического или видеоконтроля, автономные радиомикрофоны или оптоэлектронные микрофоны с вынесенными излучающими элементами и др.

Наиболее сложные и соответственно самые дорогие – **специальные технические средства,** позволяющие перехватывать информацию на некотором удалении от ее источника.

Это:

- регистраторы виброакустических колебаний стен и систем коммуникаций, возникающих при разговоре в помещении;
- регистраторы ослабленных акустических полей, проникающих через естественные звуководы (например, системы вентиляции);
- регистраторы побочных излучений от работающей оргтехники;
- направленные и высокочувствительные микрофоны для контроля речевой информации от удаленных источников;
- средства дистанционного визуального или видеоконтроля;
- лазерные средства контроля вибраций оконных стекол и др.

Специальные закладные устройства, устанавливаемые в СВТ.

Под **аппаратной закладкой** понимают электронное устройство, скрытно устанавливаемое (внедряемое) в СВТ с целью обеспечить утечку информации, нарушение ее целостности или блокирование.

Аппаратная закладка, как правило, состоит из:

- блока перехвата;
- блока передачи информации (или модуля записи информации);
- блока ДУ (при необходимости);
- блока питания.

Блок перехвата подключается к информационным кабелям или к платам блоков СВТ и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приемный пункт.

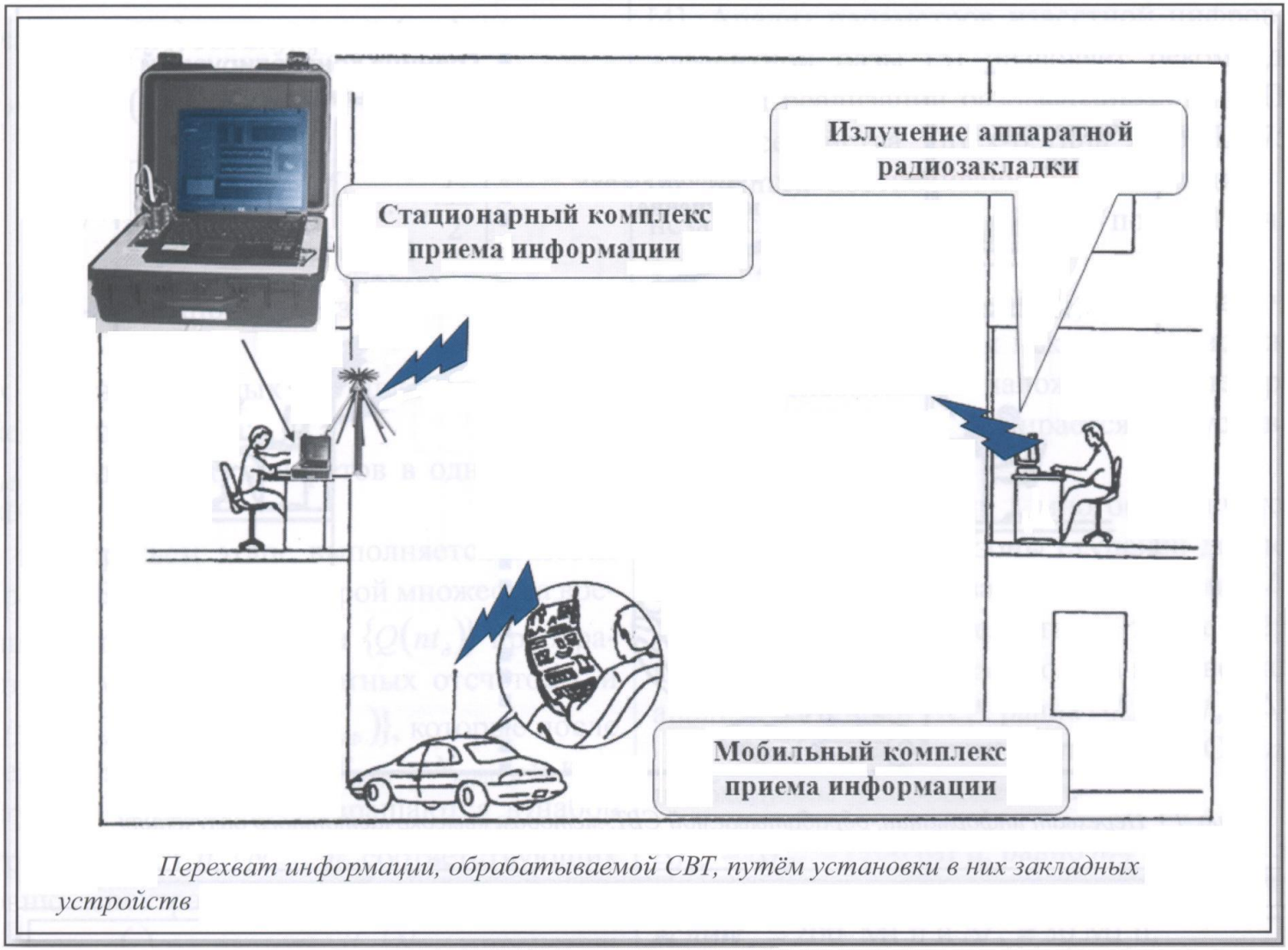
Перехватываемая аппаратными закладками информация может записываться в память ЗУ (например, на flash-память) или передаваться на приемный пункт по радиоканалу, электросети, выделенной линии, оптическому каналу (при использовании ИК-порта) и т.п.

С помощью системы ДУ осуществляется включение/выключение устройства (запуск программы перехвата информации), включение/выключение режима передачи информации, установка параметров процесса съема и передачи информации.

Классификация закладных устройств, устанавливаемых в СВТ.

Показатель классификации	Значения
Вид перехватываемой информации	1. Видеоизображение, выводимое на экран монитора. 2. Информация, вводимая с клавиатуры. 3. Информация, выводимая на принтер. 4. Информация, записываемая на жесткий диск компьютера (HDD). 5. Информация, записываемая на внешние накопители (flash-память, CD, DVD, USB-накопители). 6. Информация, передаваемая по каналу связи.
Место установки	1. В корпусе системного блока. 2. Подключаемые к внешним разъемам системного блока (например, USB). 3. Подключаемые в виде переходных элементов в разрыв информационных кабелей, соединяющих системный блок с оконечными устройствами, например, клавиатурой, принтером и т.п. 4. В корпусе монитора. 5. В корпусе клавиатуры. 6. В корпусе принтера. 7. В корпусе модема и т.п.
Способ передачи информации	1. Без передачи информации (перехваченная информация записывается на специальные цифровые накопители, например, на flash-память). 2. По радиоканалу. 3. По сети 220 В. 4. По выделенной линии. 5. По оптическому каналу.
Средство передачи информации	1. Специальное радиопередающее устройство. 2. ИК-порт. 3. Устройства типа Bluetooth. 4. Устройства типа Wi-Fi, WiMAX и т.д.
Тип источника питания	1. От низковольтных источников питания технических средств. 2. От сети 220 В.
Вид исполнения	1. Обычные (отдельные модули). 2. Камуфлированные под типовые элементы электронных устройств.
Способ управления передатчика	1. Неуправляемые (с включением передатчика при включении СВТ). 2. Дистанционно управляемые.
Способ накопления информации	1. Без накопления. 2. С промежуточным накоплением (с коротким и длительным временем накопления).
Способ кодирования информации	1. Без кодирования информации. 2. С цифровым шифрованием информации.

Принцип перехвата информации, обрабатываемой СВТ, с помощью установки в них специальных закладных устройств.



Перехват информации, обрабатываемой СВТ, путём установки в них закладных устройств

Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ (аппаратные кейлоггеры).

Аппаратные кейлоггеры (***keylogger hardware***) являются самыми распространёнными закладными устройствами и предназначены в основном для перехвата паролей пользователей и текстовых документов, набираемых с использованием ПЭВМ.

Данные устройства могут подключаться в разъем между системным блоком и клавиатурой (изготавливаются в виде переходников или удлинительных кабелей), а так же скрытно устанавливаться в корпусе клавиатуры или внутри системного блока с подключением к интерфейсу клавиатуры.

Перехватываемая информация может передаваться на контрольный пункт в режиме реального времени по радиоканалу или записываться на flash-память.

Существуют модели кейлоггеров с накоплением, которые по внешней команде передают записанную информацию по радиоканалу (в том числе, используя технологию Wi-Fi).

Принцип работы аппаратного кейлоггера с записью информации на flash-память, устанавливаемого в разъем между клавиатурой и системным блоком ПЭВМ.

Аппаратные кейлоггеры с записью информации на flash-память состоят из датчика, осуществляющего перехват сигналов, передаваемых от клавиатуры в системный блок, микроконтроллера и модуля памяти. Такие кейлоггеры не требуют дополнительного питания и работают под управлением любой ОС. Кейлоггер записывает все нажатия клавиш в собственную память, в специальный файл (обычно формата ".txt"). После того, как память кейлоггера заполнится, он прекращает запись информации.

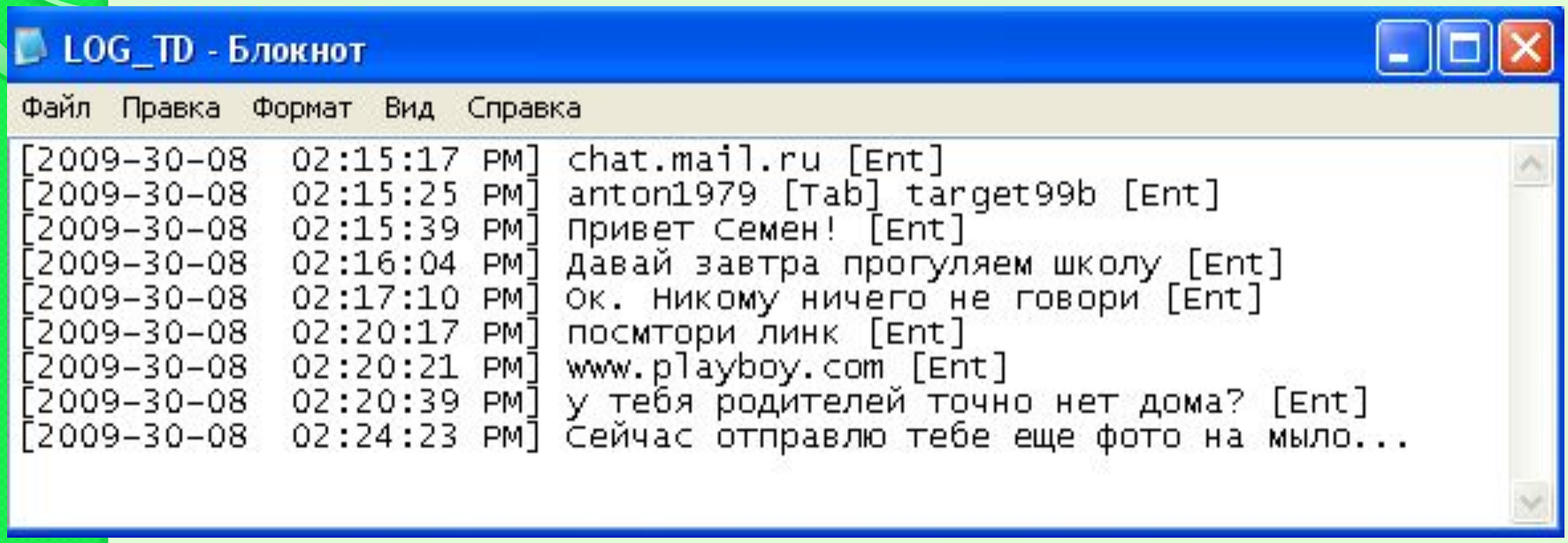
Встроенная память на 2Гб позволяет осуществлять непрерывную запись информации в течение полутора лет без ее очистки.

Варианты аппаратных кейлоггеров, устанавливаемых между клавиатурой и системным блоком ПЭВМ.

В зависимости от конкретной модели кейлоггер имеет следующие основные характеристики:

- Запись информации осуществляется на flash-память объёмом от 64 Кб до 2 ГГб. Объём памяти 1 МГб обеспечивает запись до 2000000 нажатий клавиш или 500 страниц текста.
- Защита памяти 128 битной системой шифрования данных.
- Возможность записи и чтения текста на различных языках.
- Возможность установки модуля, позволяющего фиксировать время и дату набранного на клавиатуре текста с точностью до секунды.
- Совместимость со всеми проводными клавиатурами соответствующего типа (PS/2 или USB).
- “Невидимость” для операционной системы, невозможность обнаружения с помощью антивирусных программ.

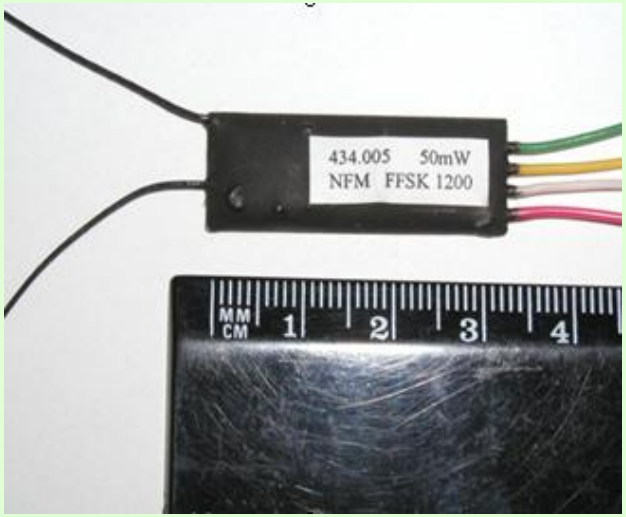
Пример файла-отчёта аппаратного кейлоггера с записью информации на flash-память.



Принцип работы аппаратного кейлоггера с передачей информации по радиоканалу, устанавливаемого в разъем между клавиатурой и системным блоком ПЭВМ.

- Аппаратный кейлоггер - это чисто электронное устройство, которое не требует установки какого-либо дополнительного ПО, вмешательства в ОС, драйверы и т.п. Однако, у большинства аппаратных кейлоггеров есть недостаток - периодически требуется физический доступ к компьютеру для “переброса” информации из памяти кейлоггера. Этого недостатка нет у так называемых “радиокейлоггеров” (Wireless Keylogger).
- Радио (или беспроводной) кейлоггер состоит из двух основных модулей: передатчика и приемника. Передатчик и приемник сделаны под PS/2 и USB удлинители с т.н. “балуном” (ферритовое кольцо - фильтр). Сам модуль кейлоггера находится в передатчике, который является PS/2 аппаратным кейлоггером с встроенным радиопередающим модулем на 2.4 ГГц. Все нажатия клавиш клавиатуры передаются в реальном времени по радиоканалу. Приемник подключен через USB-порт к другому компьютеру, на котором с помощью специального ПО отображаются принятые данные.
- Вся система работает в режиме реального времени: текст, который набирается на клавиатуре с передатчиком, сразу же виден на приемной стороне. Максимальный радиус действия составляет около 50 метров. В здании с 3-4 стенами радиус действия составляет около 20 метров (зависит от толщины стен).

Принцип работы аппаратного кейлоггера с передачей информации по радиоканалу, скрытно устанавливаемого в клавиатуру ПЭВМ.



Кейлоггер **KS-1** - Keyboard Transmitter:

- Предназначен для перехвата информации, набираемой на клавиатуре типа PS/2.
- Устанавливается в клавиатуру ПК и передает информацию о нажатых клавишах по радиоканалу в цифровом виде (FFSK).
- Рабочая частота находится в диапазоне 430 МГц. Мощность передатчика 50 мВт, что обеспечивает дальность передачи на несколько сотен метров.
- Комплект состоит из самого кейлоггера **KS-1** и приемного оборудования (специальный приёмник, модем и ПО).
- Не обнаруживается антивирусными программами.

Аппаратные закладки для перехвата информации, выводимой на монитор ПЭВМ (аппаратные видеологгеры).

Видеологгер - это аппаратная закладка миниатюрных размеров, установленная в обычный видео кабель, соединяющий системный блок ПК с монитором.

Данное устройство подключается к **DVI, VGA** или **HDMI** порту компьютера и незаметно делает снимки экрана с заданной периодичностью, сохраняя их на встроенную flash-память в формате JPEG.

Для просмотра собранных скриншотов видеологгер подключается к USB порту через специальный USB ключ (входит в комплект). После этого устройство определится как новый съемный диск, на котором находится папка со снимками экрана в формате JPEG. Снимки содержат информацию о дате и времени сделанных скриншотов.

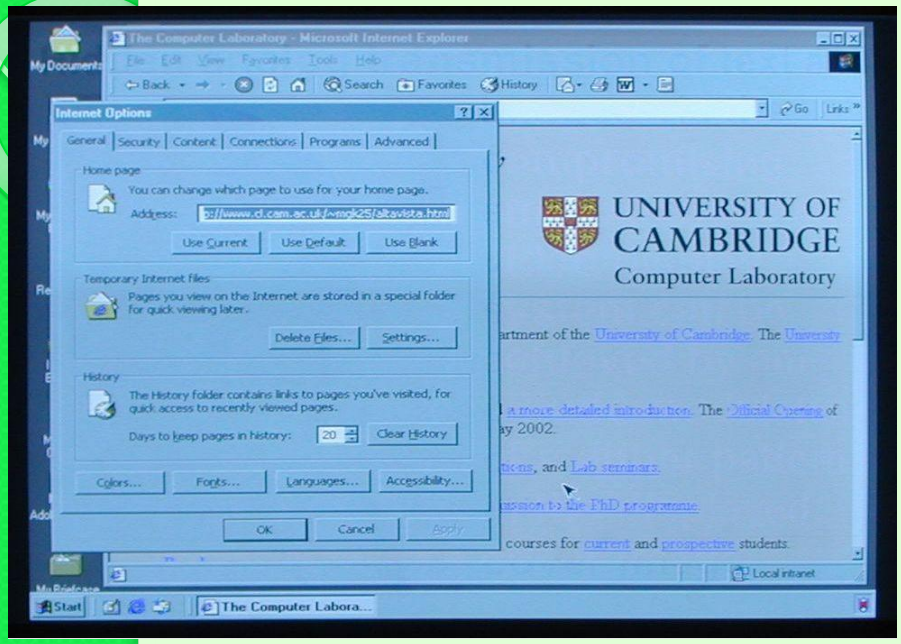
Основные характеристики типового аппаратного видеологгера.

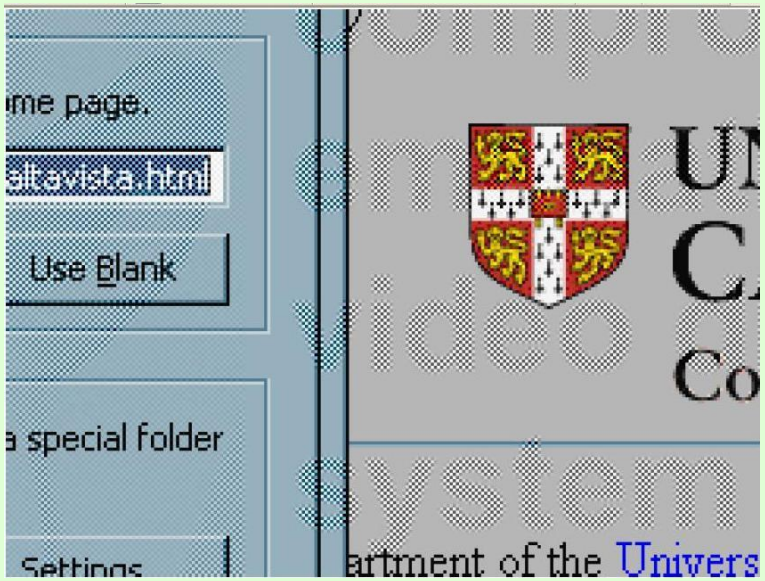
- Совместим с разъемами **DVI, HDMI, VGA**.
- Поддерживает разрешение до Full-HD (1920 x 1080), а также WUXGA (1920 x 1200).
- Совместим со стационарными ПК и внешними мониторами, подключенными к ноутбукам.
- Не требует дополнительного питания (питается через USB шнур от USB порта).
- Встроенный JPEG кодировщик .
- 2 Гб встроенной памяти.
- Имеет встроенный модуль даты и времени с независимым источником питания (гарантийный срок службы 7 лет).
- Не требует установки драйверов, совместим с Winows, Linux и Mac OS.
- Имеет небольшие размеры и высокий уровень камуфляжа - выглядит как внешний мини кабель для монитора.
- Не обнаруживается антивирусными программами.

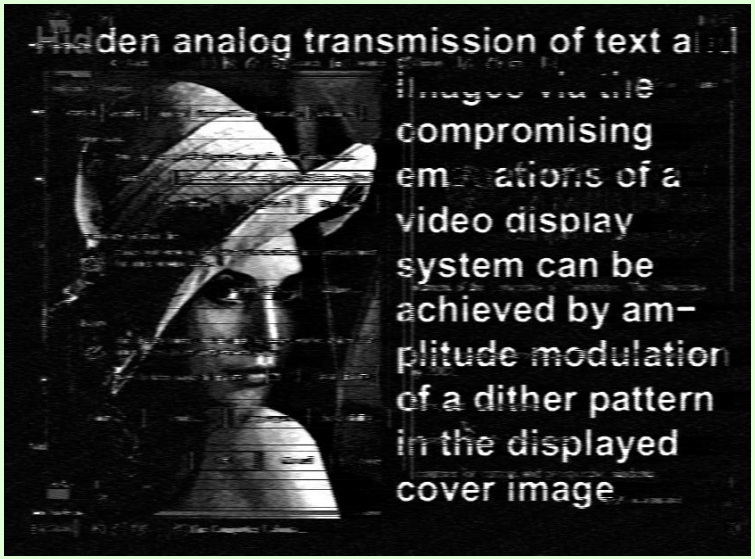
Использование технологии Soft Tempest для получения информации, обрабатываемой СВТ.

- Технология **Soft Tempest** – это технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью специальных программных средств. Данная технология заключается в том, чтобы целенаправленно управлять излучением компьютера с помощью специальных программных закладок.
- Технология **Soft Tempest** является разновидностью компьютерной стеганографии, т.е. метода скрытной передачи нужного (информативного) сообщения в обычных видео, аудио, графических и текстовых файлах (“файлах-контейнерах”).
- Принцип реализации данной технологии следующий: нужный компьютер “заражается” специальной “программой-закладкой”, а затем данная программа ищет необходимую информацию на диске и путем обращения к различным устройствам компьютера вызывает появление побочных излучений, содержащих нужный информативный сигнал. Например, учеными из Кембриджа была разработана “программа-закладка”, которая “встраивала” информативное сообщение в композитный сигнал монитора. При этом были подобраны такие характеристики управляющих сигналов, что информация, излучаемая в эфир, отличалась от отображаемой на экране монитора.
- Если в качестве изображения, играющего роль стегоконтейнера, выбрать “обои” рабочего стола, то такое изображение не вызывает подозрений у пользователя компьютера, несмотря на то, что в это время в эфир излучается найденная “программой-закладкой” информация. Хотя методы Soft Tempest атаки, предложенные учеными Кембриджа, имели ряд недостатков – для передачи полезного сигнала используется сигнал монитора, что требует выполнения определенных условий (оператор должен использовать “нужную” экранную заставку, передача возможна при перерывах в работе оператора и т.д.) – они наглядно продемонстрировали реальность данного канала утечки информации.

Образцы изображений, полученных с помощью перехвата ПЭМИ, возникающих при использовании технологии Soft Tempest .







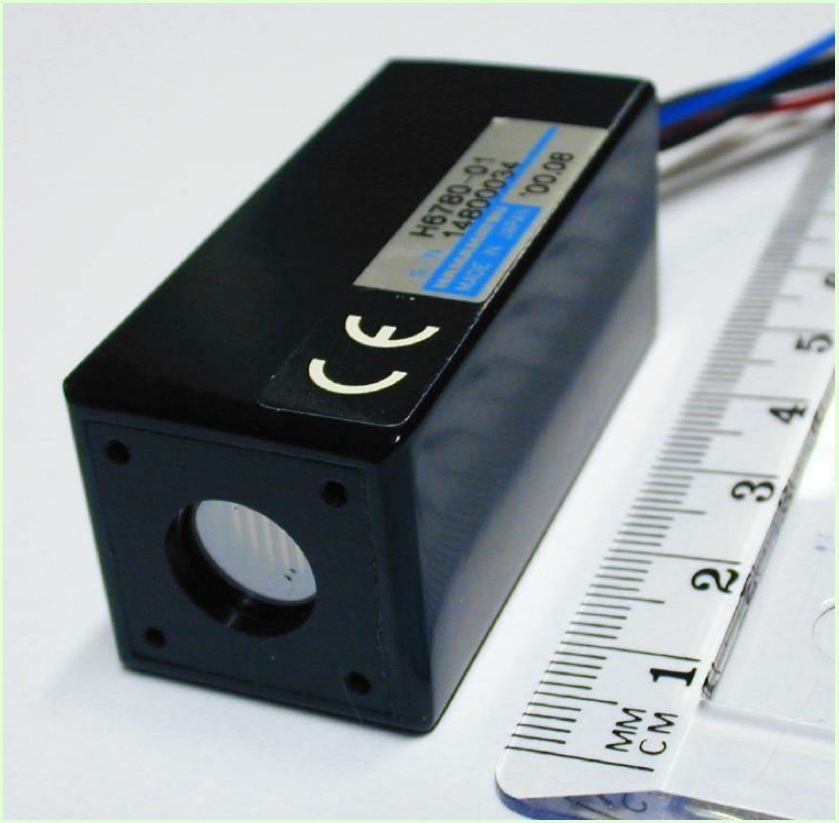
Восстановление изображения на мониторе ПК с помощью приёма переотражённого светового излучения монитора.

Одним из реальных каналов утечки информации, обрабатываемой на ПК, является визуальное наблюдение за экраном монитора.

Монитор ПК должен быть размещён таким образом, чтобы информация на его экране была недоступна для просмотра посторонними лицами.

Однако световой поток от экрана монитора отражается от стен, и этот отраженный световой поток тоже может быть перехвачен.

В различных источниках (*см. список литературы*) было заявлено об успешных экспериментах по восстановлению изображения, принятого после его многократных отражений от стен и других окружающих предметов – *хотя <u>лично для меня</u> это непонятное “явление” как такое может быть*.



The Hamamatsu H6780-01 photosensor module used for these experiments contains a photomultiplier tube together with a high-voltage power supply.

Образцы изображений, полученных с помощью приёма переотражённого светового излучения монитора.