Технические каналы утечки информации, обрабатываемой средствами вычислительной техники.

Фантомэ А.В.
инженер, техническая защита информации

Кишинёв
2015

Термины и определения.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации в соответствии с заданной информационной технологией, а так же помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены.

Объекты информатизации, на которых обработка информации осуществляется с использованием средств вычислительной техники (СВТ), называют “**объектами СВТ**”.

Защищаемый объект информатизации (объект защиты) – объект информатизации, предназначенный для обработки важной информации с обеспечением требуемого уровня ее защиты.

При рассмотрении объекта СВТ, как объекта защиты от утечки информации по техническим каналам, его необходимо рассматривать как объект, включающий в себя:

- технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа (**ТСОИ** - **ОТС**), вместе с их соединительными линиями (совокупность проводов и кабелей, прокладываемых между отдельными ТСОИ и их элементами);

- вспомогательные технические средства и системы (**ВТСС**) вместе с их соединительными линиями;

- посторонние проводники;

- систему электропитания;

- систему заземления.

Безопасность информации – состояние защищенности информации, при котором с требуемым уровнем обеспечены ее конфиденциальность, целостность и доступность.

Угроза безопасности информации – потенциальная или реальная возможность нарушения безопасности информации, обрабатываемой с помощью технических средств.

Термины и определения.

- **Техническое средство обработки информации (ТСОИ)** – техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и (или) передачи информации по каналам связи. К ТСОИ относятся средства вычислительной техники, средства и системы связи, средства звукозаписи, звукоусиления и звуковоспроизведения, средства видеозаписи и видеовоспроизведения, средства изготовления и размножения документов и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и (или) передачей информации по каналам связи.
- **Основные технические средства обработки информации (ОТС)** – средства вычислительной техники и их коммуникации, входящие в состав объекта информатизации и осуществляющие обработку, хранение и передачу важной информации.
- **Вспомогательные технические средства и системы (ВТСС)** – технические средства и системы, не предназначенные для обработки важной информации, но на которые могут воздействовать электромагнитные поля побочных излучений основных технических средств, в результате чего на ВТСС наводится опасный сигнал, который может распространяться за пределы контролируемой зоны. К ВТСС относятся средства и системы связи, измерительное оборудование, системы пожарной и охранной сигнализации, системы электрочасофикации, системы радиотрансляции, системы электроосвещения, бытовые электроприборы и т.д. ВТСС играют роль “случайных антенн”.

Термины и определения.

- **Техническая разведка** – деятельность по получению важной (защищаемой) информации с помощью технических средств.
- **Средство технической разведки** – аппаратура технической разведки, размещенная на стационарном или мобильном объекте (помещении, транспортном средстве и т.д.), и обслуживаемая соответствующим персоналом.
- **Аппаратура технической разведки** – совокупность технических устройств, предназначенных для обнаружения, приема (перехвата), регистрации и обработки сигналов, содержащих важную (защищаемую) информацию.
- **Возможности технической разведки** – характеристики способности обнаружения, распознавания, приема и регистрации информативных сигналов (ПЭМИН) средствами технической разведки.
- **Зона разведдоступности** – пространство вокруг объекта, в пределах которого реализуются возможности технической разведки.
- **Модель технической разведки** – описание средств технической разведки, содержащее их технические характеристики и тактику применения в объеме, достаточном для оценки возможностей технической разведки.
- **Информативный (опасный) сигнал** – электрические или электромагнитные сигналы и поля, по параметрам которых может быть раскрыта информация, обрабатываемая с помощью технических средств.

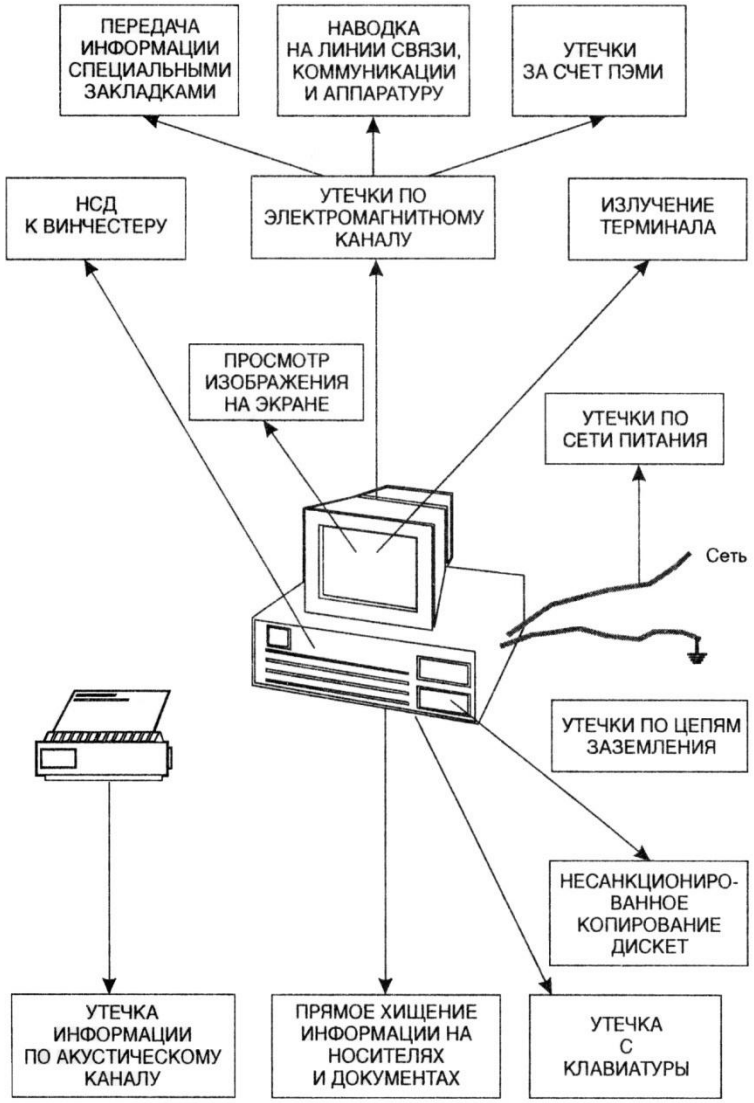
Классификация угроз безопасности информации

Формы утечки информации.

Возможные варианты утечки информации, обрабатываемой СВТ.

Для информации, обрабатываемой СВТ, актуальны все ранее перечисленные формы утечки, например:

- **Разглашение информации**: передача носителя информации постороннему лицу ***(преднамеренное)*** или обработка информации на СВТ в присутствии посторонних лиц ***(непреднамеренное)***.
- **НСД к информации**: вскрытие системного блока СВТ и изъятие HDD диска для копирования ***(физический)***, сброс установленных параметров BIOS и изменение приоритета последовательности загрузки носителя с последующей загрузкой альтернативной операционной системы и копированием интересующей информации на flash-накопитель ***(программно-аппаратный)***, внедрение в СВТ вредоносных программ для осуществления НСД к информации или её копирования ***(программный)***.
- **Хищение носителей информации**.
- **Утечка информации по техническим каналам**.



Модель каналов утечки информации и способов несанкционированного доступа ПЭВМ

Понятие технического канала утечки информации.

- **Под техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки, технического средства разведки (**ТСР** - **СТР**), 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 информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.
- Совокупность источника информативного сигнала (в данном случае - СВТ), технического средства осуществляющего перехват информации и физической среды, в которой распространяется информативный сигнал, называется ***техническим каналом утечки информации***.

В зависимости от природы образования информативного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые:

- **Естественные каналы утечки информации** образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (***электромагнитные каналы утечки информации***), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и посторонних проводниках (***электрические каналы утечки информации***)
- К **специально создаваемым каналам утечки информации** относятся каналы, создаваемые путём внедрения в СВТ электронных устройств перехвата информации (закладных устройств) и путём “высокочастотного облучения” СВТ.

Определение СТС.

Постановлением Правительства РМ № 100 от 9 февраля 2009 г. дано определение специальным техническим средствам, предназначенным для негласного получения информации: технические и/или программные средства, разработанные, приспособленные или запрограммированные для съема, получения, перехвата, сбора, прослушивания, регистрации и передачи акустических, видовых, электромагнитных и других сигналов с целью получения негласного доступа к информации, в том числе циркулирующей в сетях электронных коммуникаций.

В соответствии с **Классификатором специальных технических средств, предназначенных для негласного получения информации** (Приложение № 2 к Постановлению Правительства РМ № 100 от 9 февраля 2009 г.) к СТС отнесены следующие технические средства:

- **п. 5** СТС для негласного перехвата и регистрации информации, циркулирующей в информационных системах и сетях передачи данных (Тарифная позиция Товарной номенклатуры Республики Молдова из 8471 49 000 и из 8517 69 900).
- **п. 6** СТС для получения несанкционированного доступа к информации, находящейся в информационных системах или на других технических средствах хранения информации (Тарифная позиция Товарной номенклатуры Республики Молдова из 8471 49 000).

СТС для негласного перехвата и регистрации информации, циркулирующей в информационных системах.

Классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники (СВТ)

Обобщенная структурная схема ТКУИ, обрабатываемой СВТ.

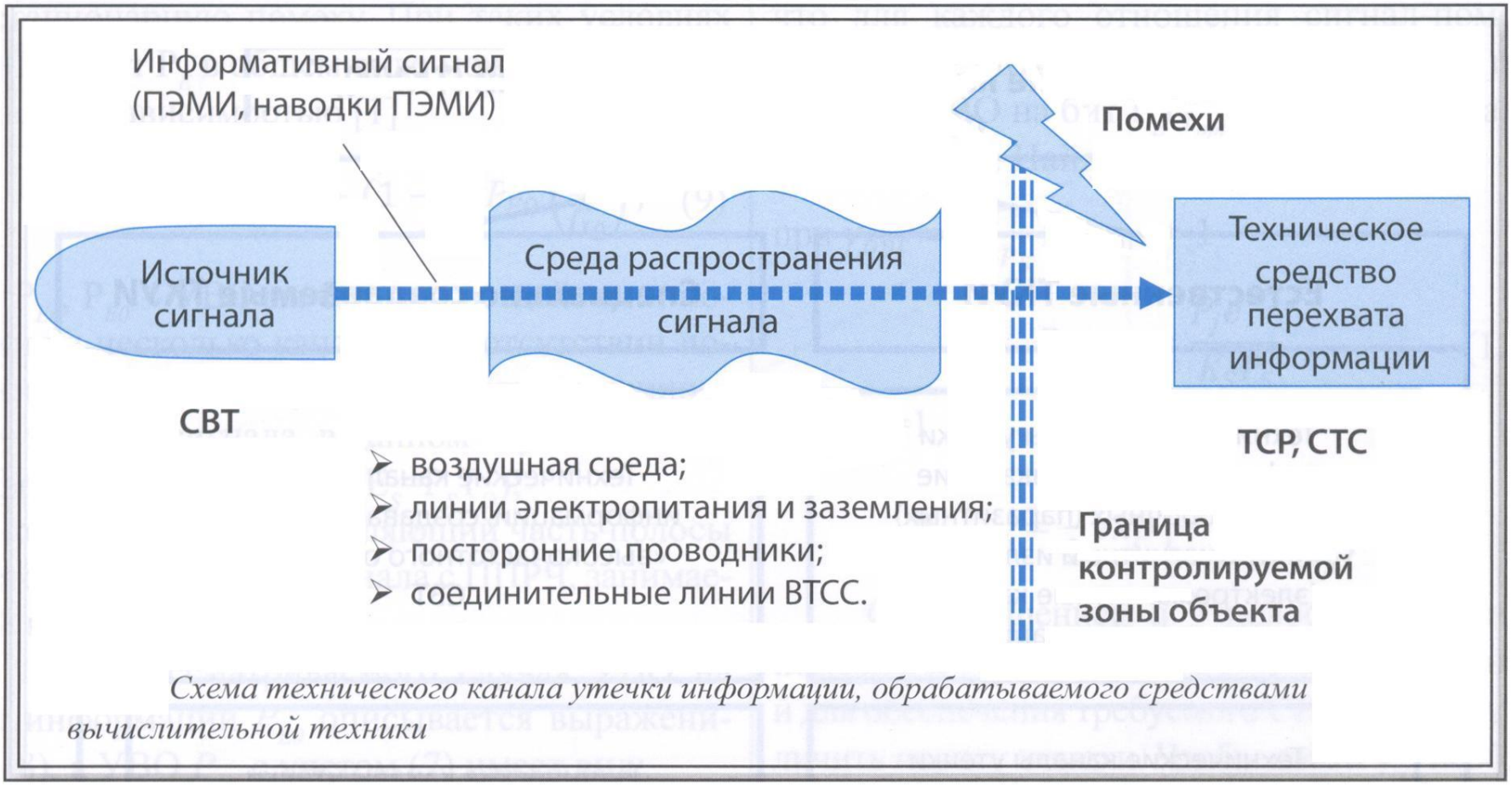


Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники

Естественные ТКУИ: электромагнитный и электрический.

В **электромагнитных каналах утечки информации** носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами.

Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ;
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

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.

Наводки информативных сигналов могут возникнуть:

- в линиях электропитания ТСОИ;
- в линиях электропитания и соединительных линиях ВТСС;
- в цепях заземления ТСОИ и ВТСС;
- в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

Понятие ПЭМИ.

- **Побочные электромагнитные излучения (ПЭМИ)** – нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации.

  С точки зрения защиты информации опасность представляют информативные ПЭМИ, содержащие в себе признаки обрабатываемой информации.
- **Информативными ПЭМИ** называются сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением выводимым на монитор, данными обрабатываемыми на устройствах ввода-вывода и т.д.).
- **Неинформативными ПЭМИ** называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ.

- ПЭМИ возникают при различных режимах обработки информации средствами вычислительной техники:
  - вывод информации на монитор;
  - ввод данных с клавиатуры;
  - запись информации на накопители;
  - чтение информации с накопителей;
  - передача данных в каналы связи;
  - вывод данных на печатные устройства;
  - запись данных от сканера и т.д.

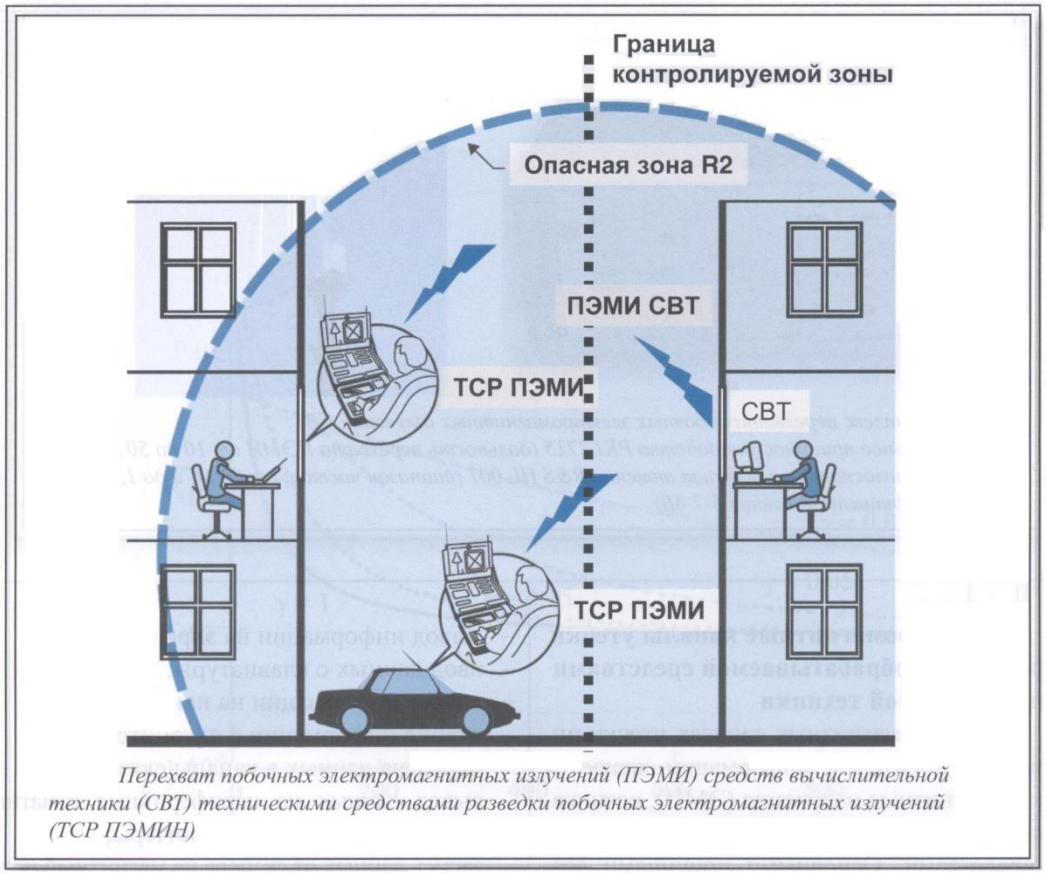
  При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности.

  Диапазон возможных частот ПЭМИ зависит от типа СВТ и может составлять от сотен Гц до десятков ГГц.

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.

Принцип перехвата ПЭМИ СВТ.



Перехват побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ) техническими средствами разведки побочных электромагнитных излучений (ТСР ПЭМИН)

- **Зона 2** (***R2***) – пространство вокруг технического средства обработки информации (объекта), в пределах которого возможен перехват побочных электромагнитных излучений и последующее восстановление содержащейся в них информации.
- В **зоне 2** отношение “сигнал/помеха” для составляющих электромагнитного поля опасного сигнала превышает допустимое нормированное значение.

Структурная схема электромагнитного ТКУИ, обрабатываемой СВТ.

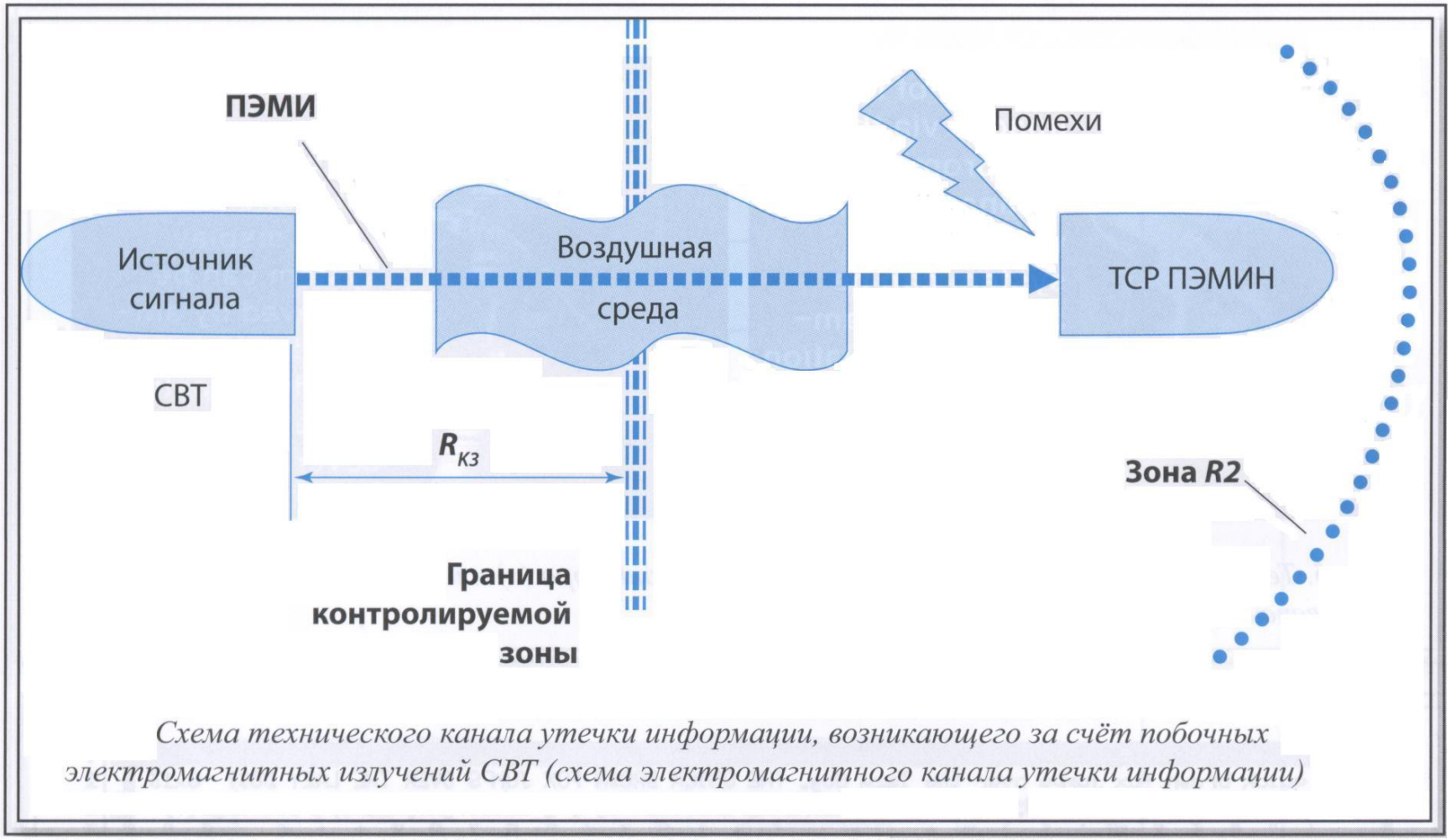
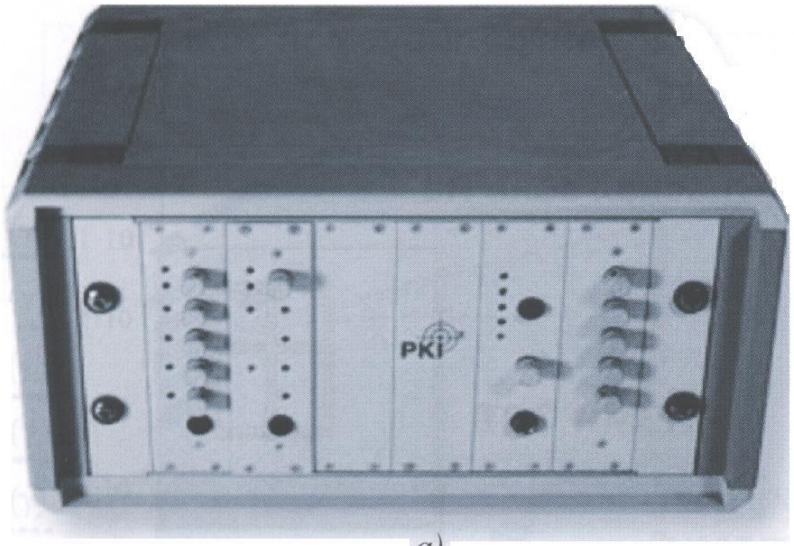
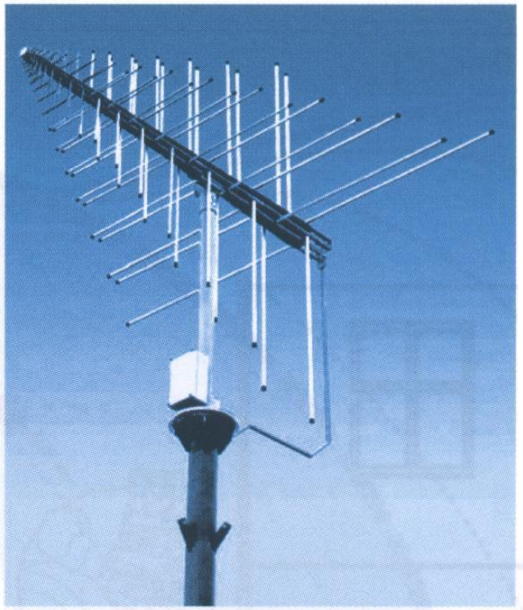


Схема технического канала утечки информации, возникающего за счёт побочных электромагнитных излучений СВТ (схема электромагнитного канала утечки информации)

Образцы оборудования для перехвата ПЭМИ.



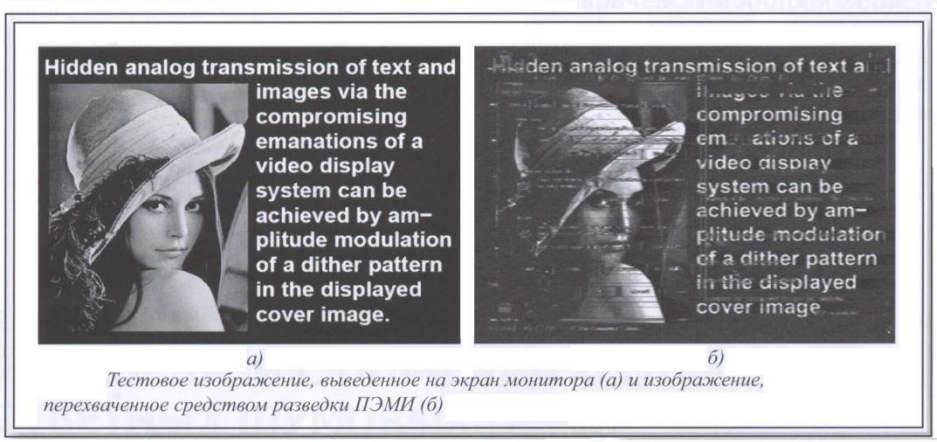
а)



б)

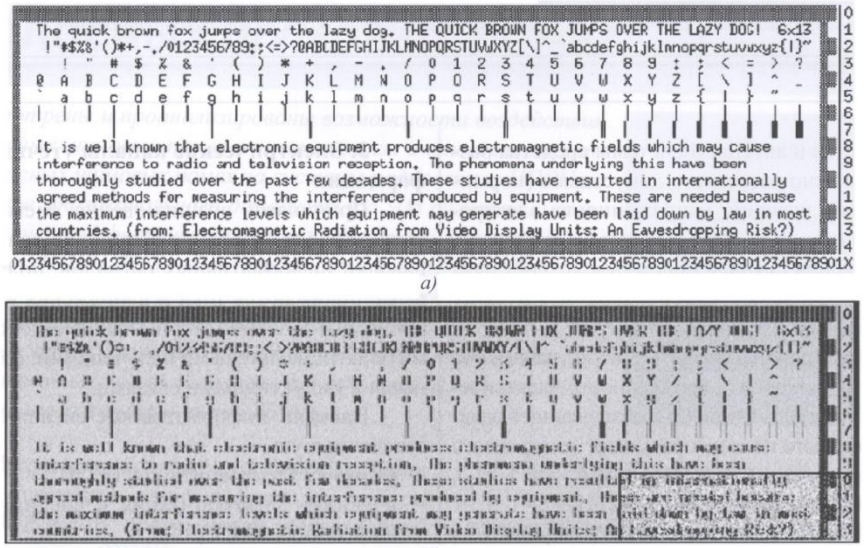
Комплекс перехвата побочных электромагнитных излучений СВТ:
а) специальное приёмное устройство PKI 2715 (дальность перехвата ПЭМИ от 10 до 50 м);
б) широкополосная направленная антенна R&S HL 007 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ)

Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.



а) *б)*

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

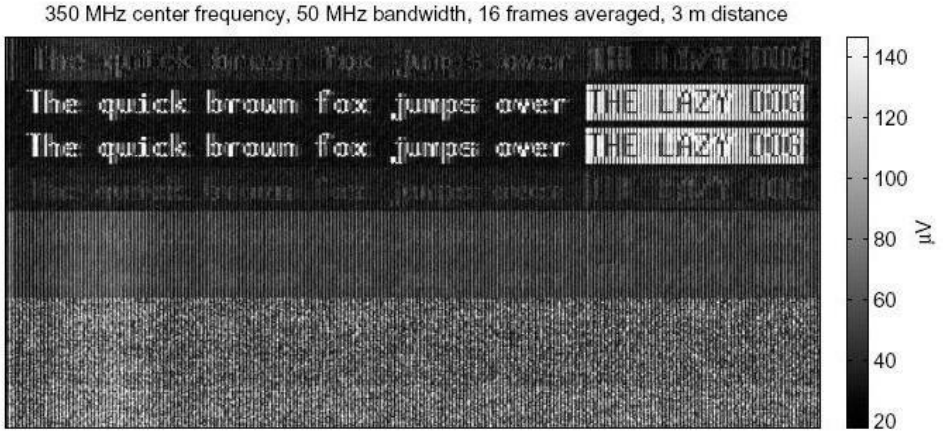


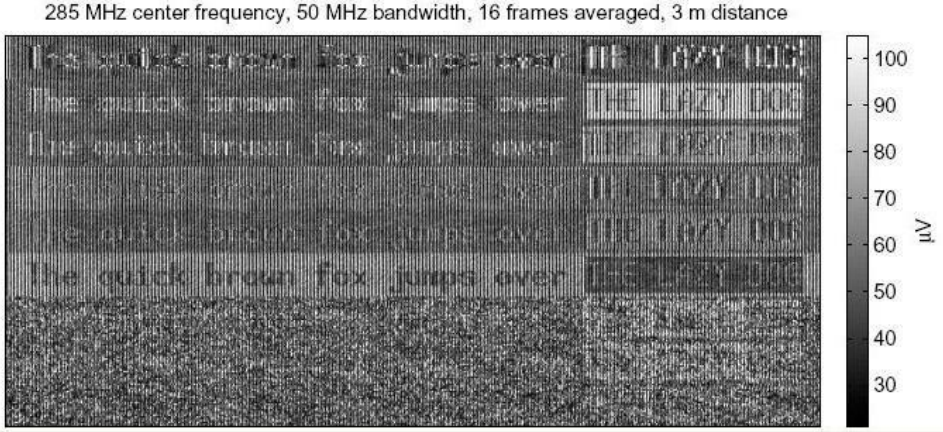
а)

б)

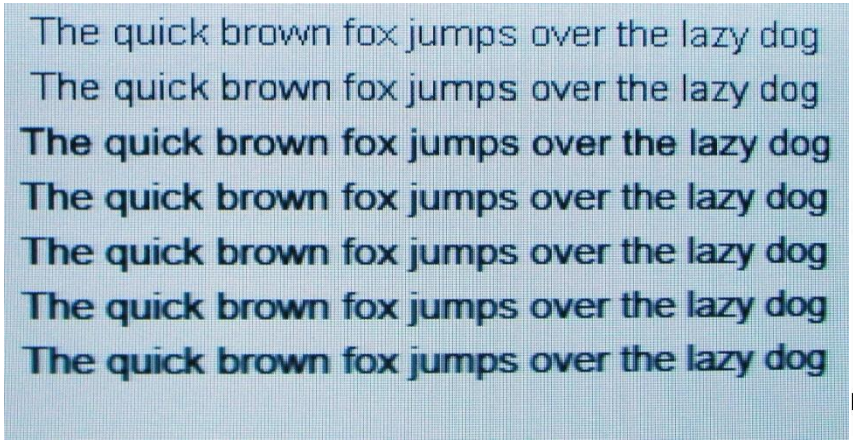
Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800×600 @ 75Hz, тактовая частота $F_т$ = 49,5 МГц, размер букв 6×13 пикселей) (а) и текст, перехваченный средством разведки ПЭМИ ($\Delta F_{пр}$ = 200 МГц) (б)

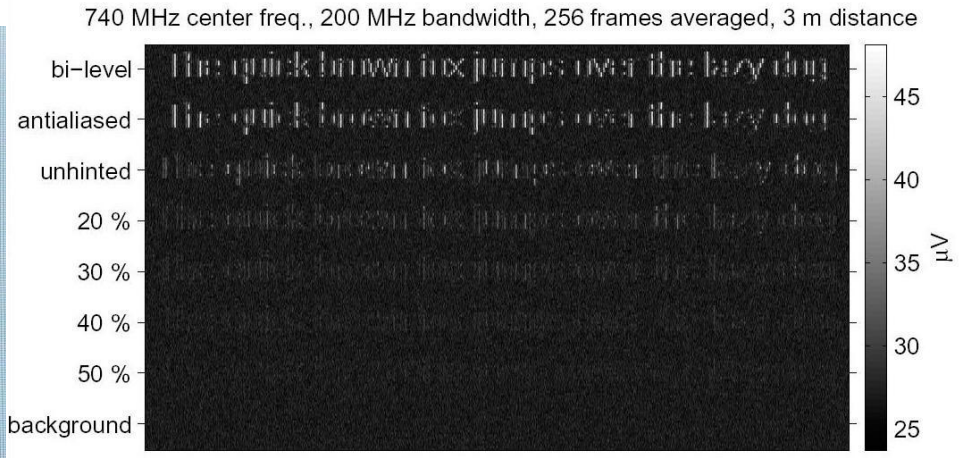
Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.





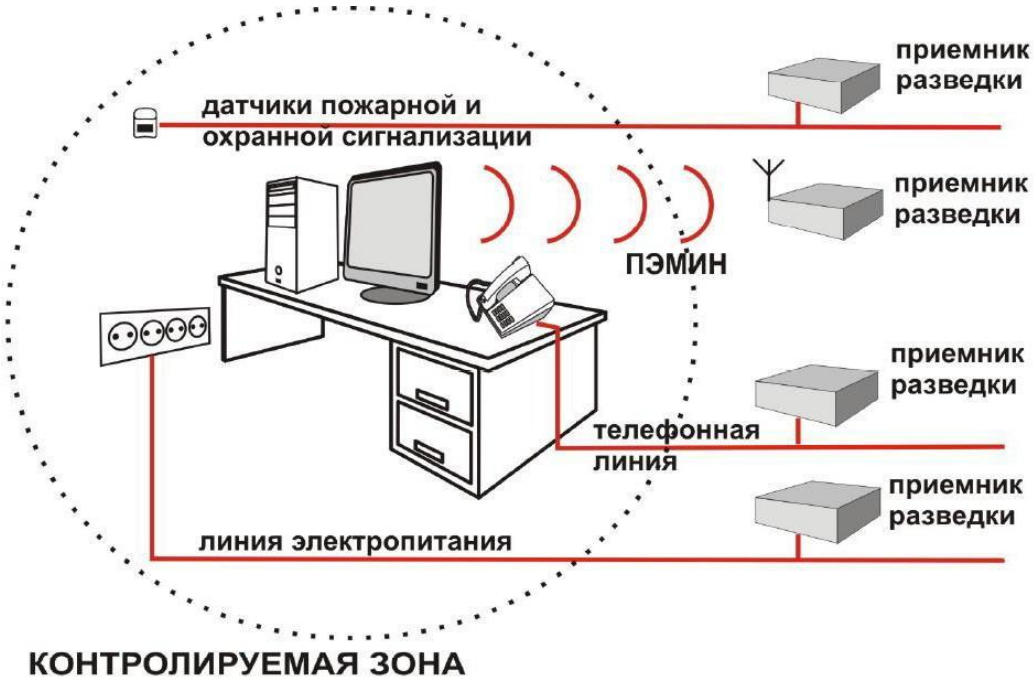
Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.





В зависимости от выбранных параметров шрифта (тип шрифта, размер букв, цвет текста и т.д.) качество перехватываемого за счёт ПЭМИ изображения будет различным.

Понятие ПЭМИН.



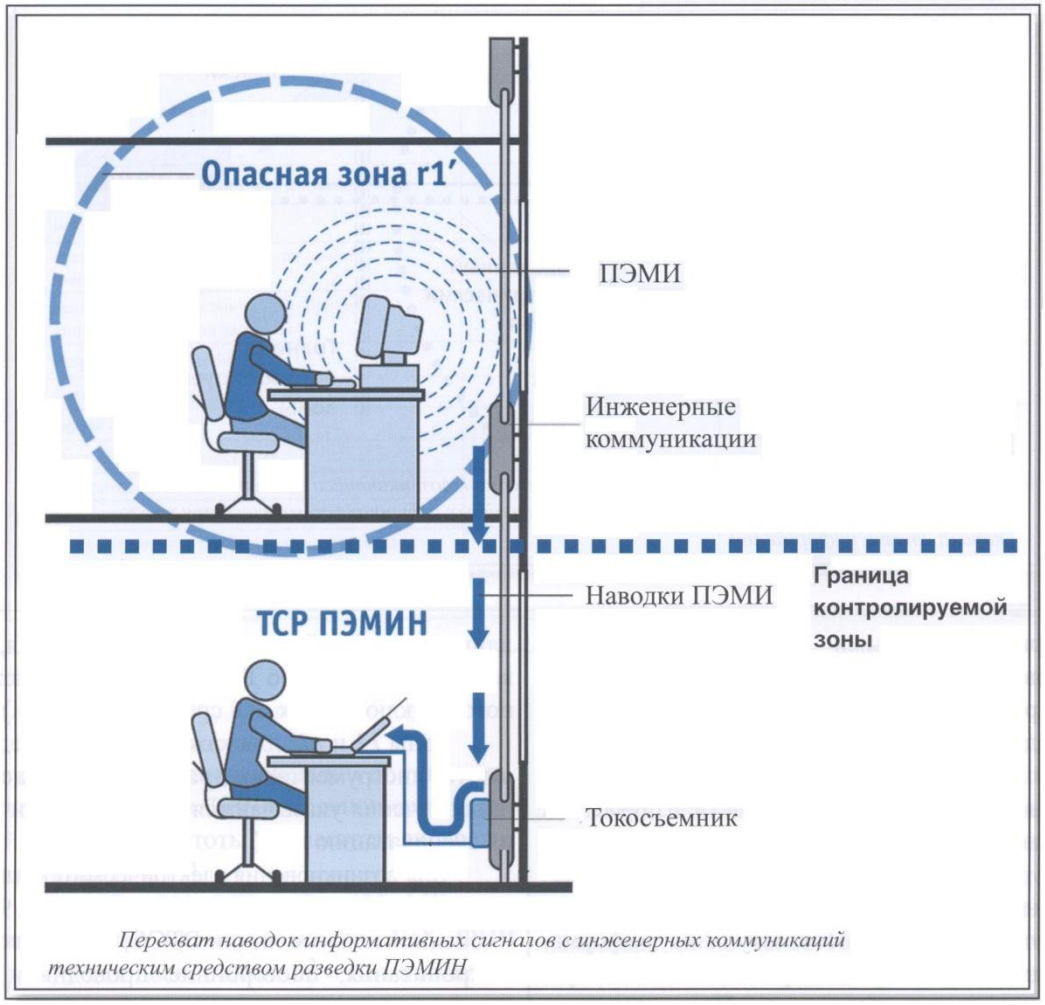
Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей.
Электромагнитные наводки могут приводить к утечке информации по токопроводящим 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, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;
- 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.

Принцип перехвата ПЭМИН СВТ.



Перехват наводок информативных сигналов с инженерных коммуникаций техническим средством разведки ПЭМИН

- **Зона 1** (***r1***)– пространство вокруг технического средства обработки информации (объекта), в пределах которого на случайных антеннах может наводиться опасный (информативный) сигнал выше допустимого (нормированного) уровня.
- В **зоне 1** запрещается размещение случайных антенн, через которые может происходить утечка важной информации за пределы контролируемой зоны.
- **Случайная антенна** – электрические и коммуникационные цепи вспомогательных технических средств и систем, а так же сами ВТСС, способные принимать побочные электромагнитные излучения.

  Случайные антенны могут быть сосредоточенными и распределенными.

Структурная схема электрического ТКУИ, обрабатываемой СВТ.

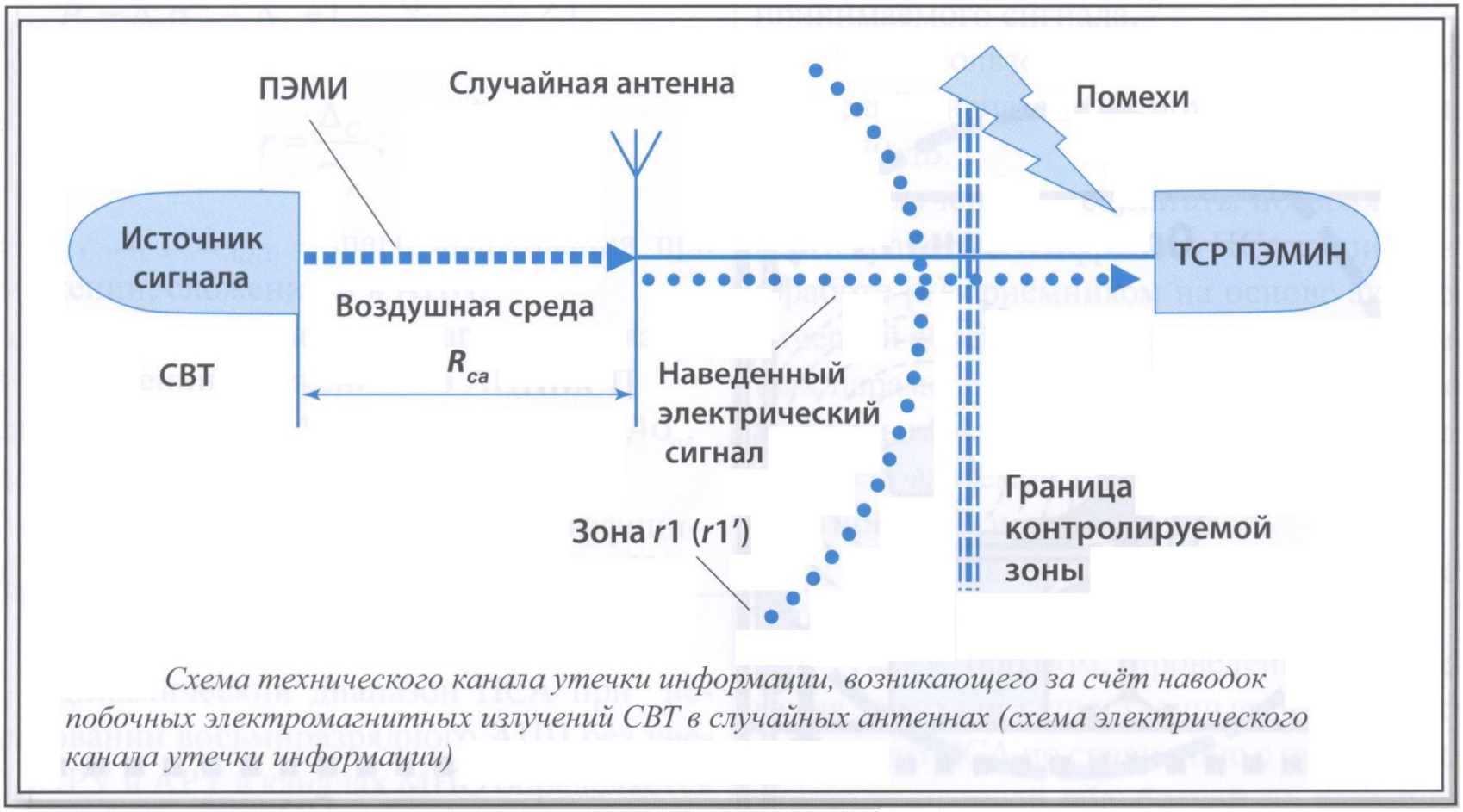
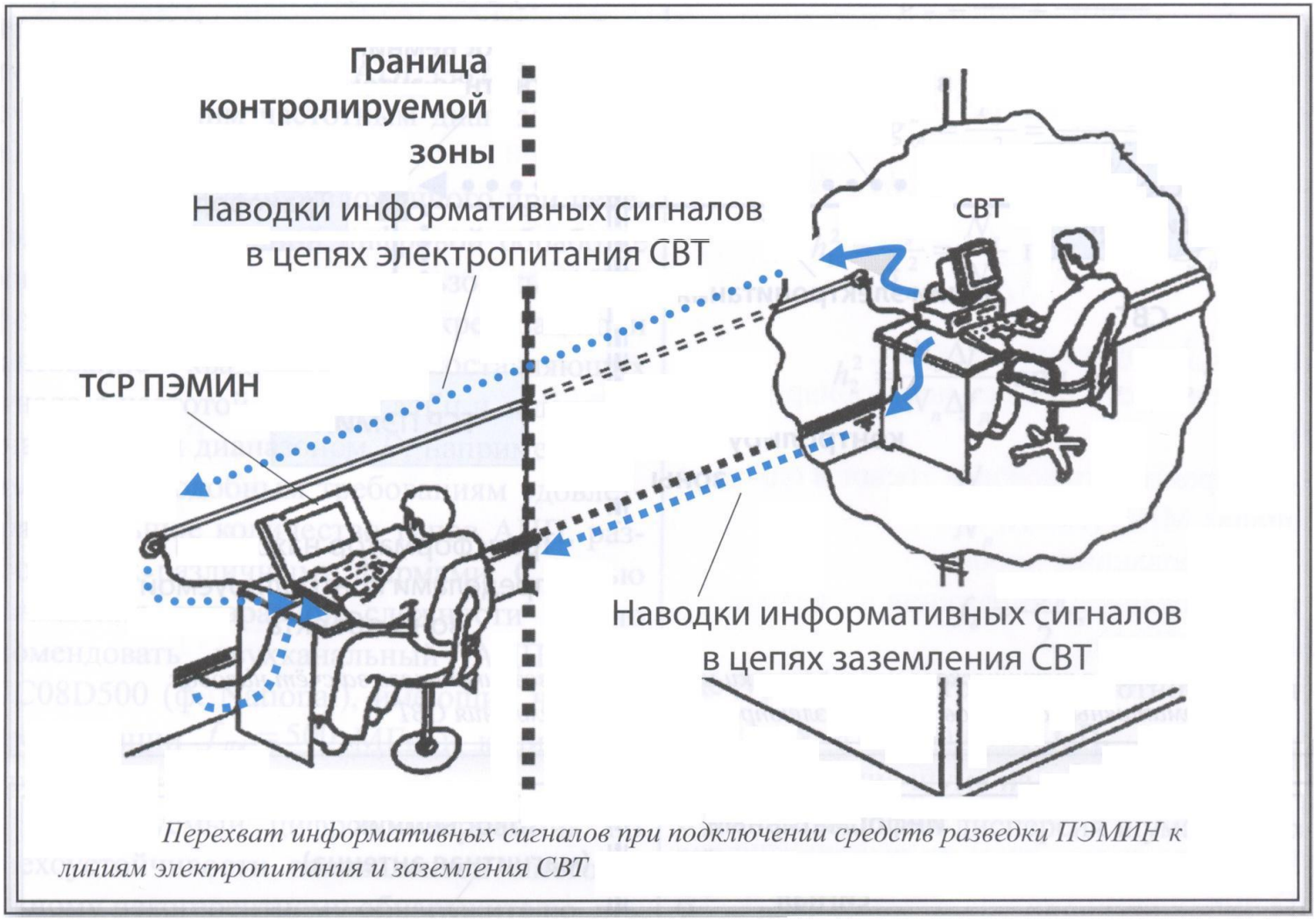


Схема технического канала утечки информации, возникающего за счёт наводок побочных электромагнитных излучений СВТ в случайных антеннах (схема электрического канала утечки информации)

Уровень наводок зависит от расстояния между источником излучения и случайной антенной, типа случайной антенны (сосредоточенная или распределённая), длиной параллельного пробега и величиной переходного затухания линий, напряжения информативного сигнала в линии и уровня шумов (помех) и других факторов.

Принцип перехвата ПЭМИН СВТ по цепям электропитания и заземления.



Перехват информативных сигналов при подключении средств разведки ПЭМИН к линиям электропитания и заземления СВТ

Структурная схема перехвата ПЭМИН СВТ по цепям электропитания.

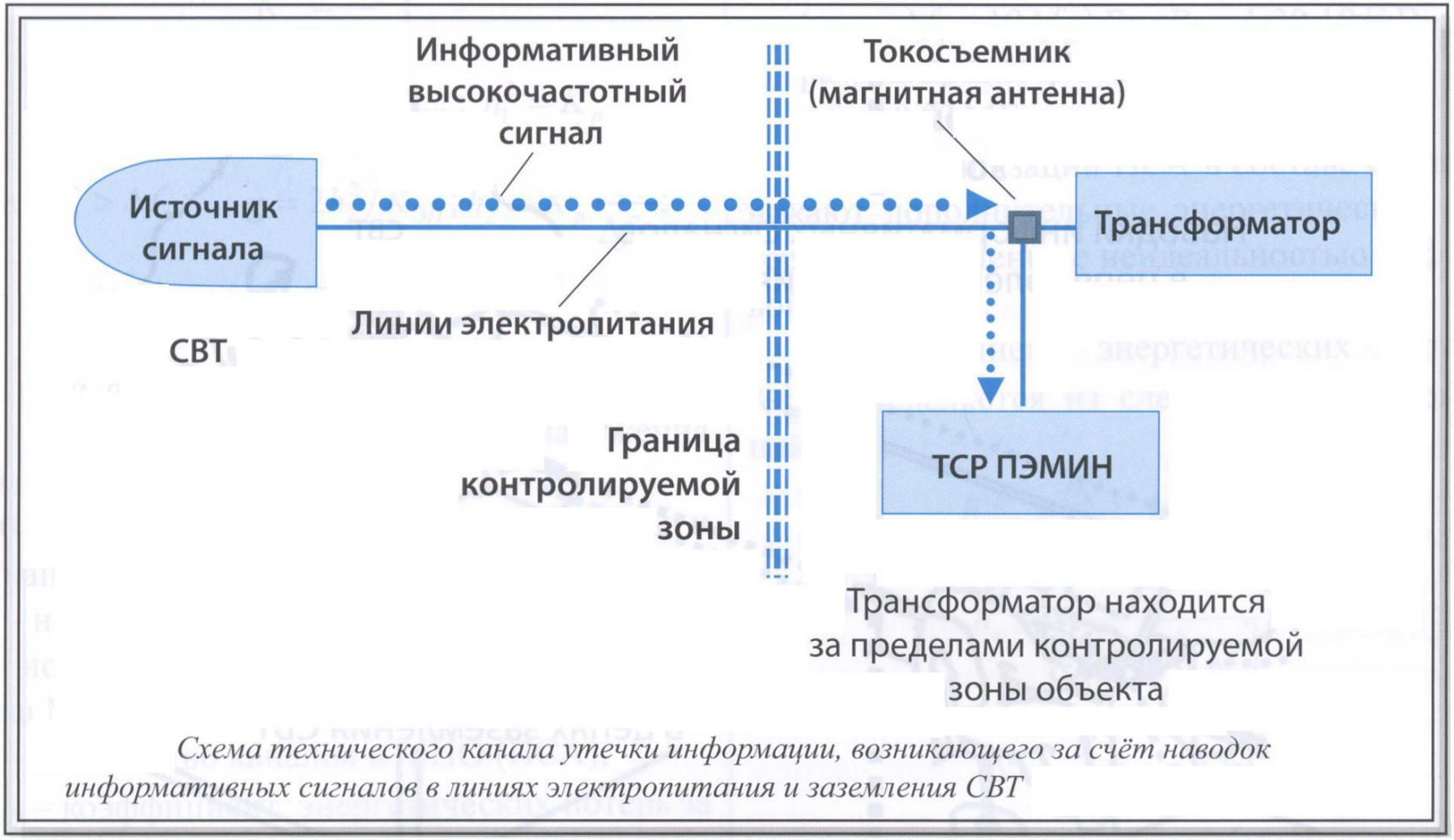


Схема технического канала утечки информации, возникающего за счёт наводок информативных сигналов в линиях электропитания и заземления СВТ

Структурная схема перехвата ПЭМИН СВТ по цепям заземления.

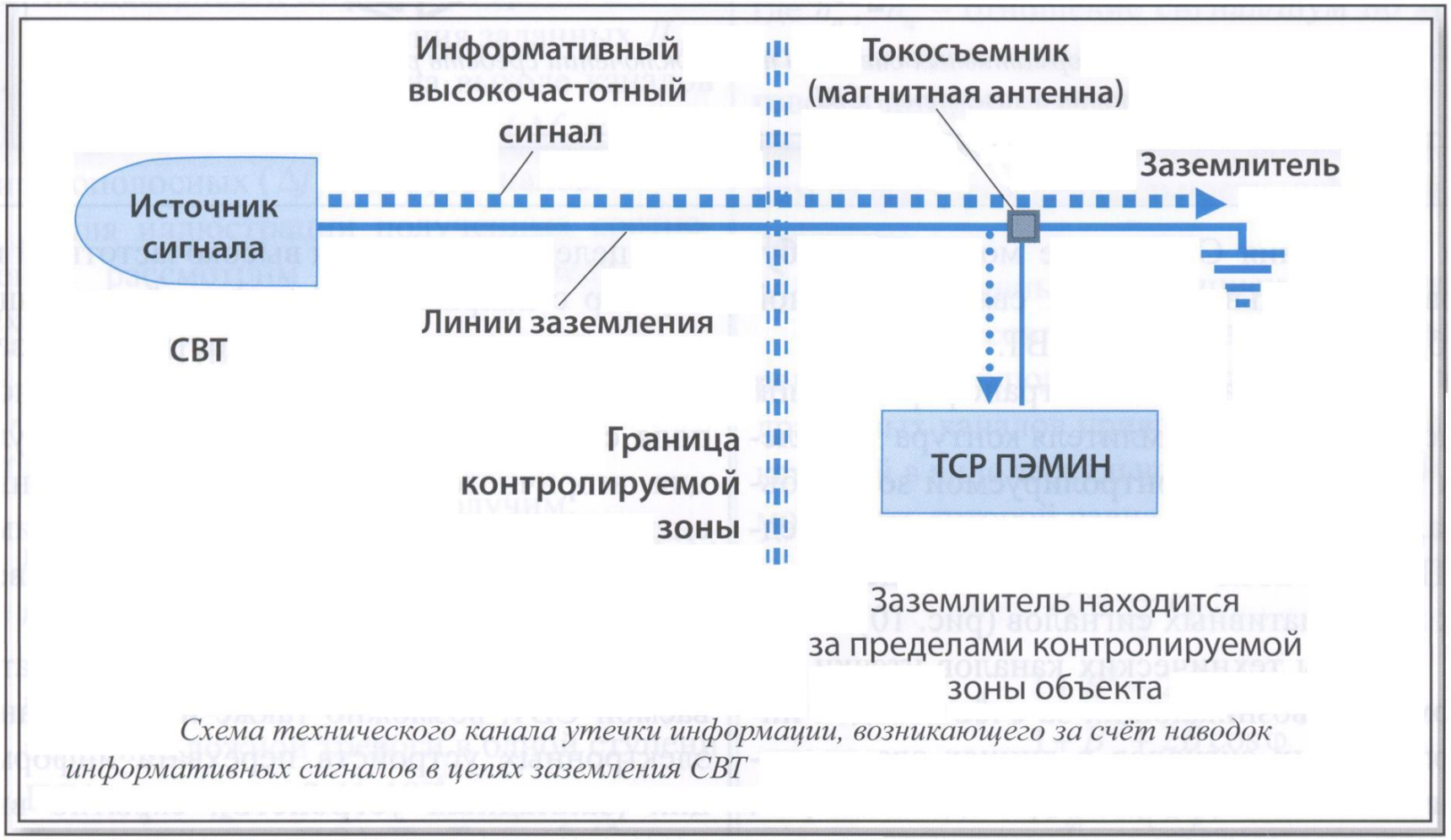
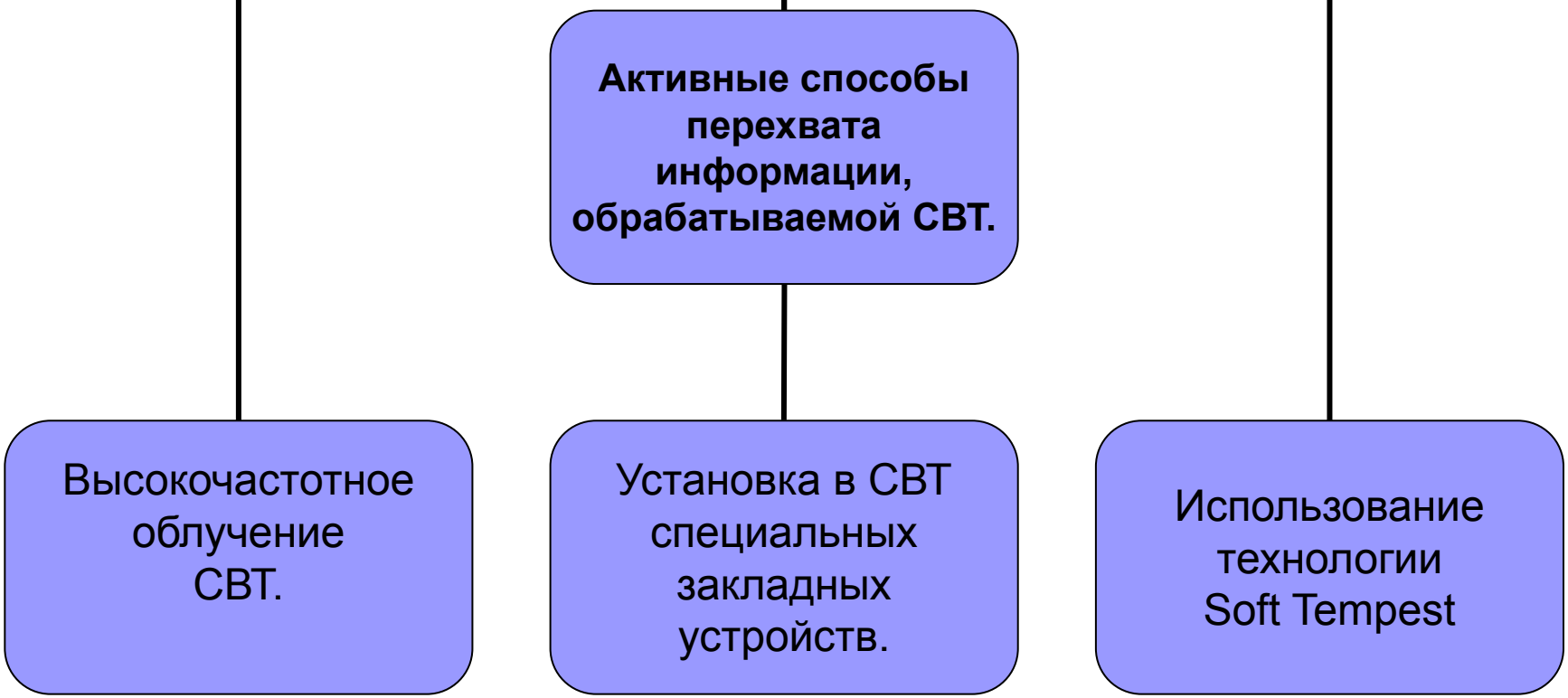


Схема технического канала утечки информации, возникающего за счёт наводок информативных сигналов в цепях заземления СВТ

Специально создаваемые ТКУИ, обрабатываемой СВТ.



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

Перехват информации, обрабатываемой СВТ, методом «высокочастотного облучения»

Структурная схема ТКУИ, создаваемого методом “высокочастотного облучения” СВТ.

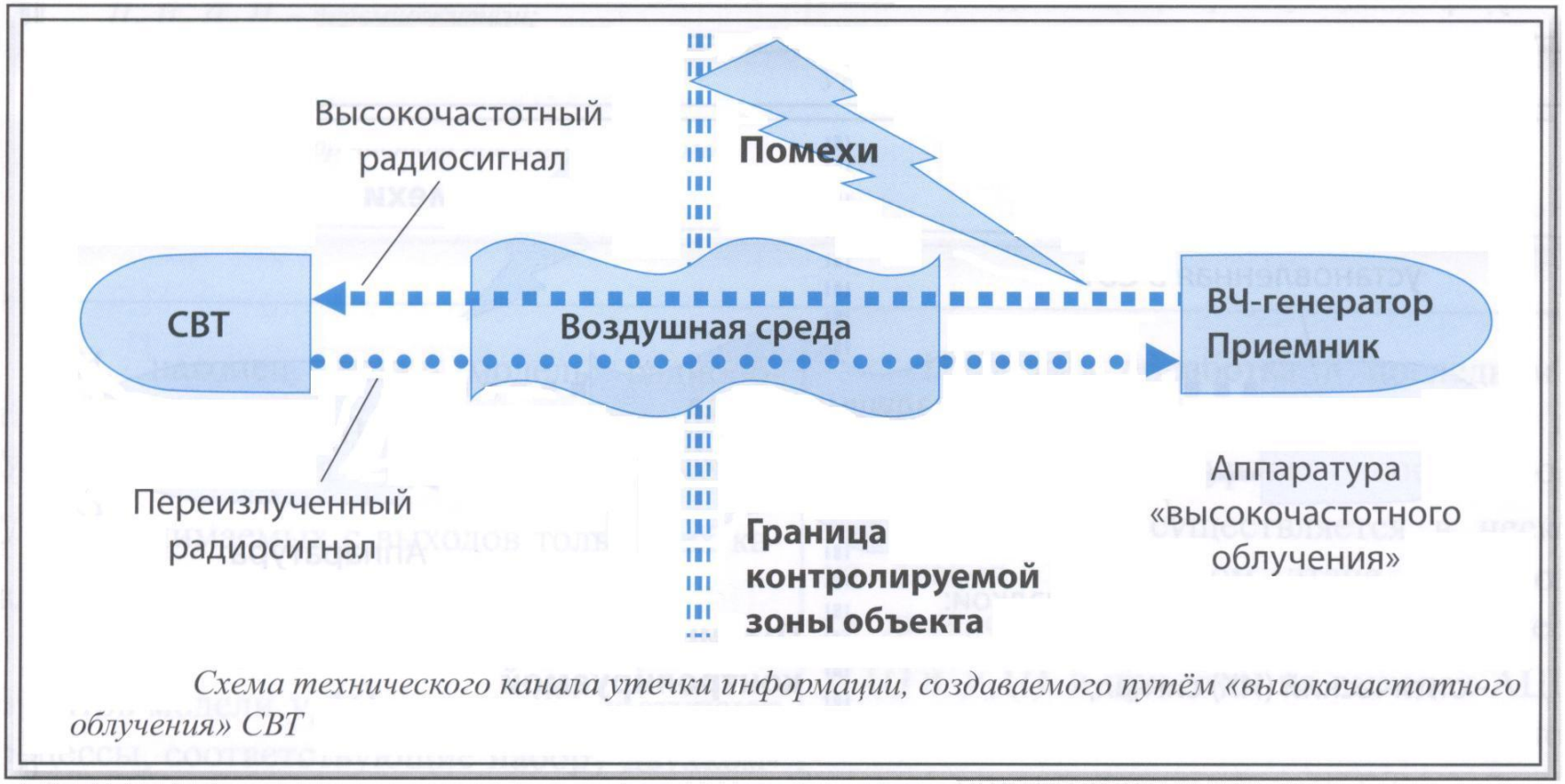


Схема технического канала утечки информации, создаваемого путём «высокочастотного облучения» СВТ

СВТ облучается мощным высокочастотным гармоническим сигналом (используется ВЧ-генератор с направленной антенной, имеющей узкую диаграмму направленности).
При взаимодействии облучающего электромагнитного поля с элементами СВТ происходит модуляция вторичного излучения информативным сигналом. Переизлучённый сигнал принимается приёмным устройством ТСР и детектируется.

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.

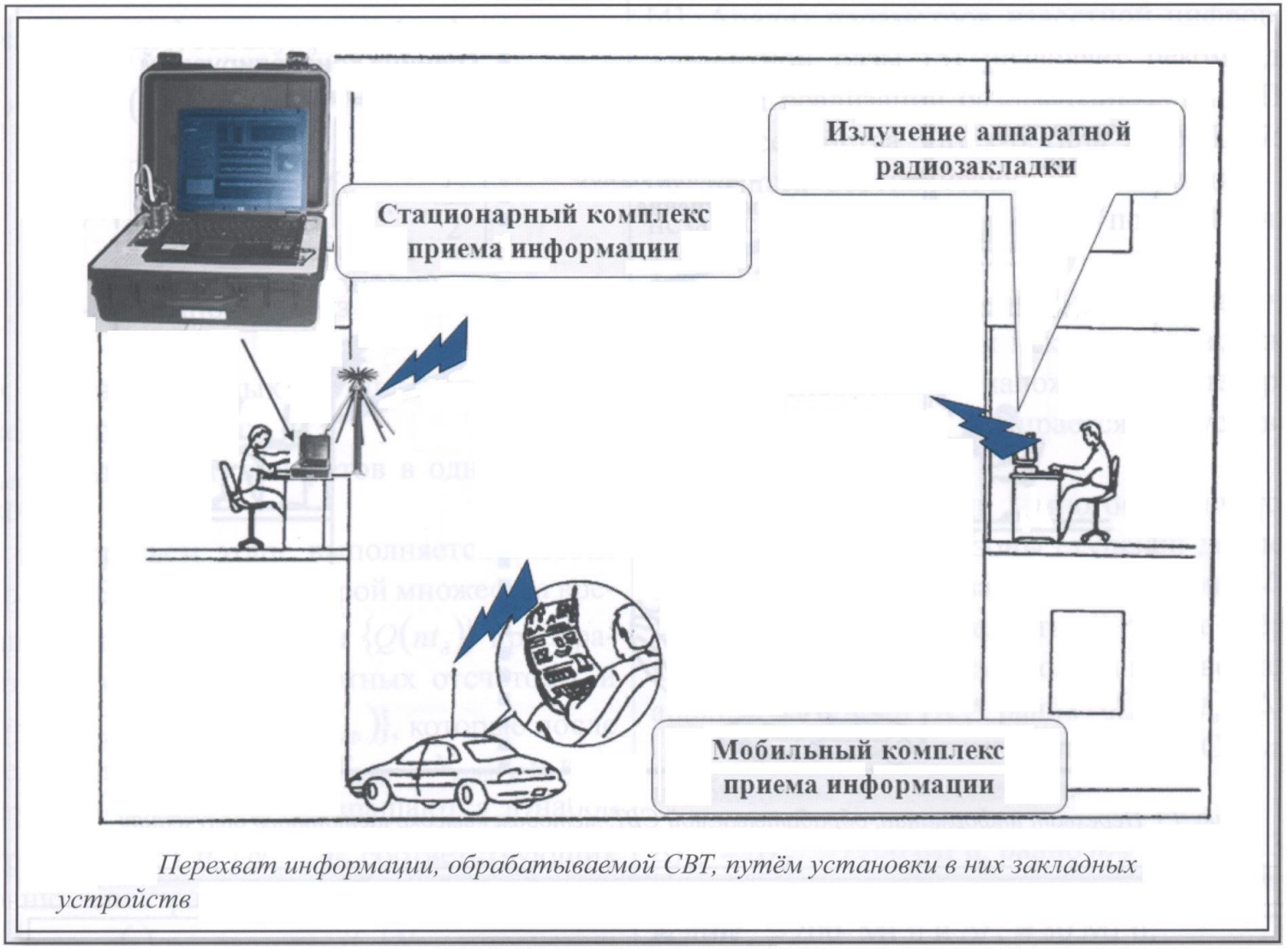
Перехватываемая аппаратными закладками информация может записываться в память ЗУ (например, на flash-память) или передаваться на приемный пункт по радиоканалу, электросети, выделенной линии, оптическому каналу (при использовании ИК-порта) и т.п.

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

Структурная схема ТКУИ, создаваемого путём установки в СВТ специальных закладных устройств.

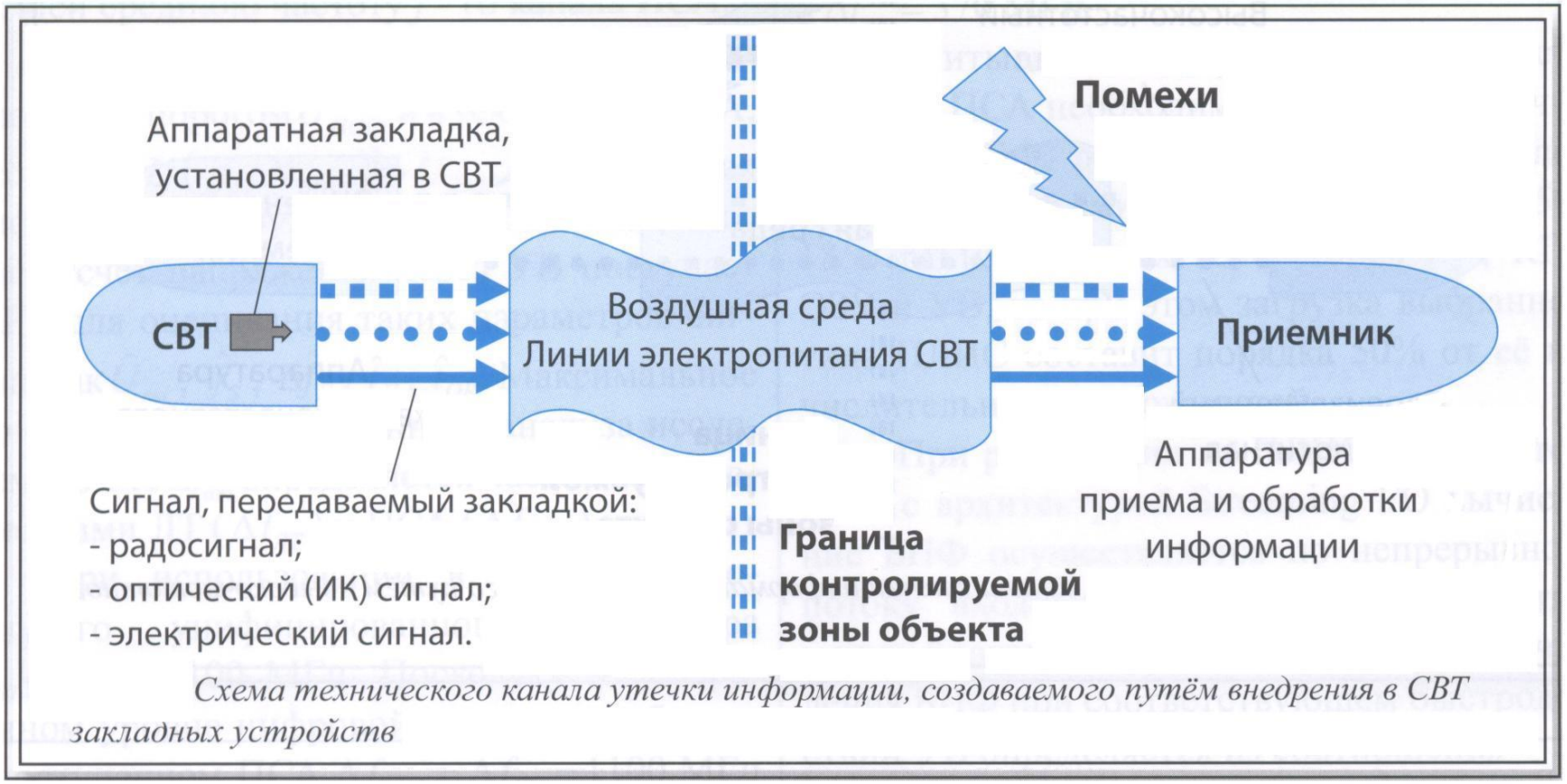


Схема технического канала утечки информации, создаваемого путём внедрения в СВТ закладных устройств

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.

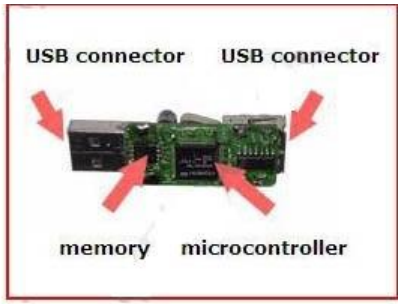
Данные устройства могут подключаться в разъем между системным блоком и клавиатурой (изготавливаются в виде переходников или удлинительных кабелей), а так же скрытно устанавливаться в корпусе клавиатуры или внутри системного блока с подключением к интерфейсу клавиатуры.

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.

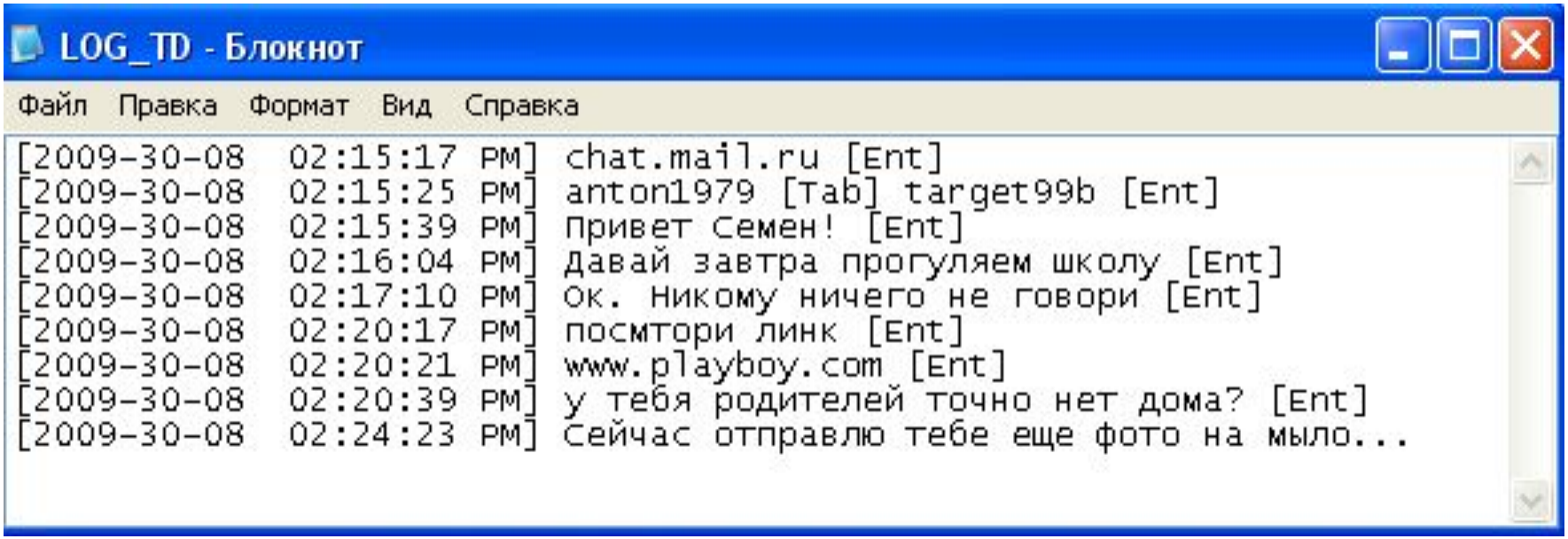


Варианты аппаратных кейлоггеров, устанавливаемых между клавиатурой и системным блоком ПЭВМ.

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.

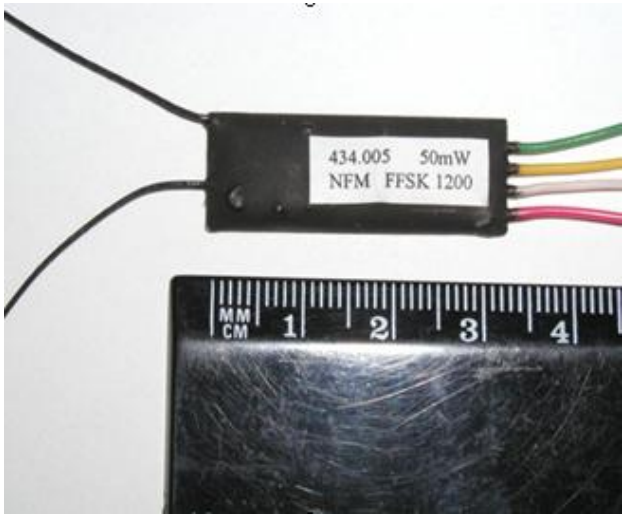
Пример файла-отчёта аппаратного кейлоггера с записью информации на flash-память.



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.

Аппаратно-программная закладка для отбора и копирования нужных файлов с ПК.

MAKE SECRET COPIES OF FILES AND DOCUMENTS FROM A PC, WHILE LEAVING NO TRACE

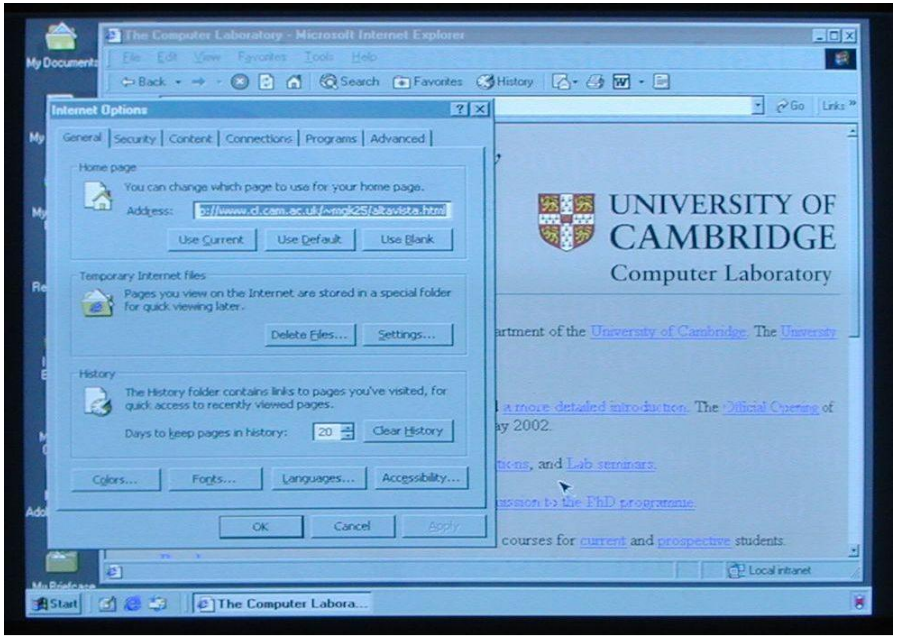
It scans a PC, and extracts the desired files and documents, in a matter of seconds!

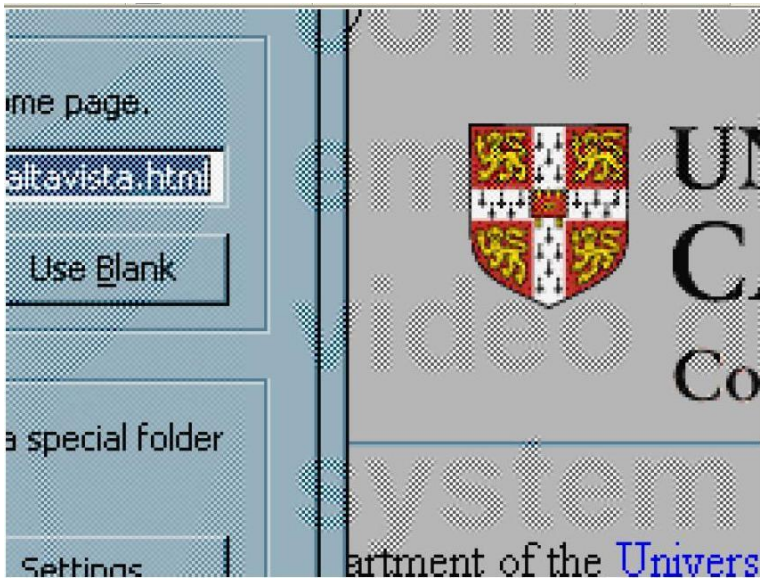
- To put your hands on files and documents without leaving any trace, our device is the absolute best choice!
  Do you need to quickly extract sensitive documentation and data files, while leaving no visible sign?
- For this purpose we have created a data extraction device, powerful and professional, and compatible with any Microsoft operating system, which can autonomously run on basically any hardware. Its quick setup and easy commands make it suitable for being used even by the less experienced of users.
- Our powerful data extractor is always ready to be used. Its operation is very simple: By connecting it to the victim's PC, all you have to do is activate it, and in a few seconds its intuitive graphic interface allows you to choose the file formats and types you wish to extract.
- Just click on OK, and the graphic interface would then disappear while the device starts to operate in discreet mode.
  A few minutes is all it takes to analyze the PC hard drive and any external drives, USB sticks, network folders, CDs or DVDs. The device would silently extract sensitive information, files, documents, emails, images, folders and so on. Like a powerful magnet, it attracts the desired information, that you will later be able to view and analyze in depth.
- It contains no trojan or malware that could be blocked by an antivirus software, as the data extraction is done discreetly and without any trace left, just thanks to its high technological level.
- What would happen if our victim suddenly returns to their computer? No problem at all, thanks to our extractor the operation can be interrupted at any time, with no error message, alert or confirmation request; everything that has been captured up to that time would remain stored in the data extraction device.
- Our data extraction device can be concealed within a 16 GB USB drive or stick, with a fast and ground-breaking 2.0 firmware. This device can extract data at the whopping speed of 480 MB/s and is the most common of its kind, in terms of ease of use and operating speed, with a 100% success ratio.
  Designed specifically for this task, it can perfectly be adapted to any PC, making it very easy to retrieve the information you are looking for.

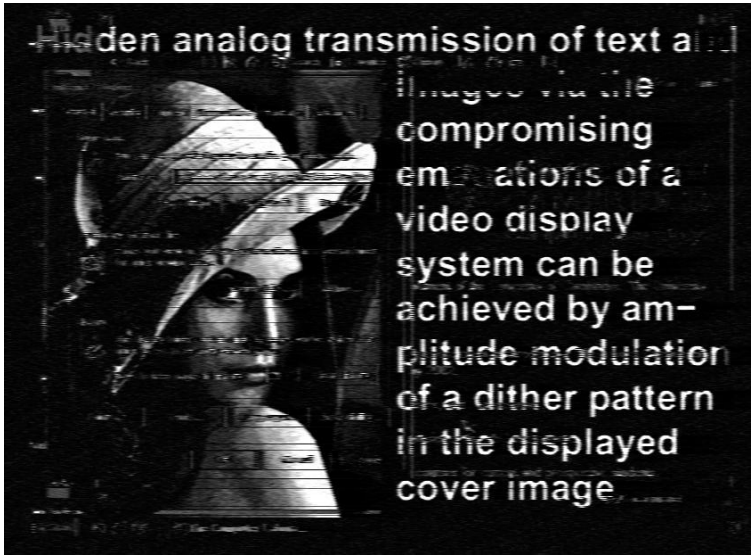
Использование технологии Soft Tempest для получения информации, обрабатываемой СВТ.

- 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 .

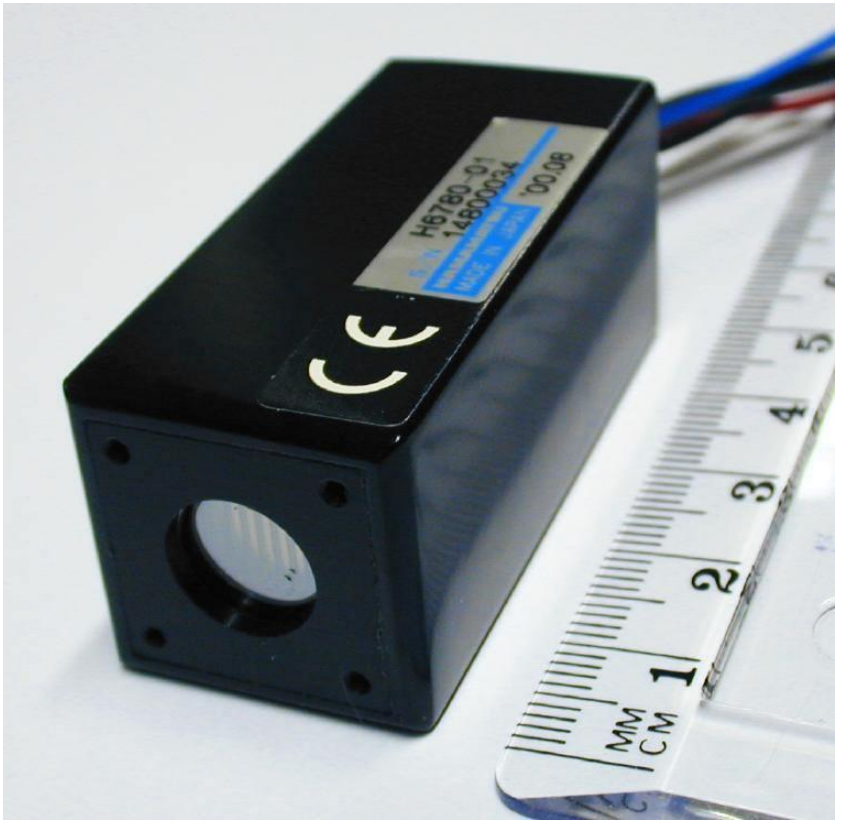






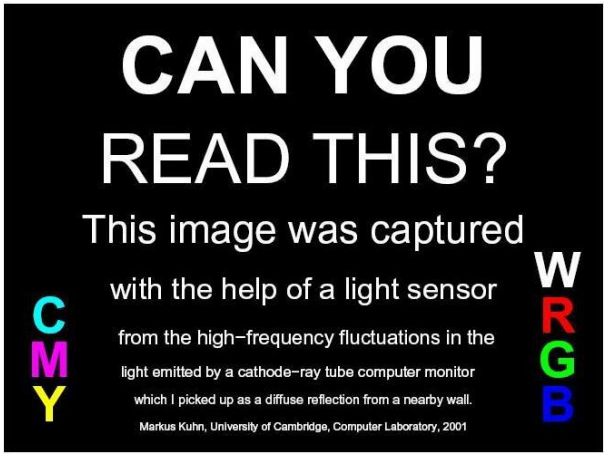
Восстановление изображения на мониторе ПК с помощью приёма переотражённого светового излучения монитора.

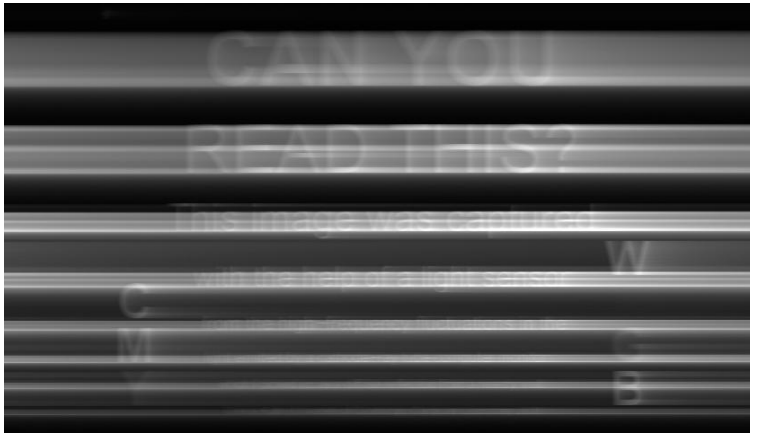
Одним из реальных каналов утечки информации, обрабатываемой на ПК, является визуальное наблюдение за экраном монитора.
Монитор ПК должен быть размещён таким образом, чтобы информация на его экране была недоступна для просмотра посторонними лицами.
Однако световой поток от экрана монитора отражается от 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*.

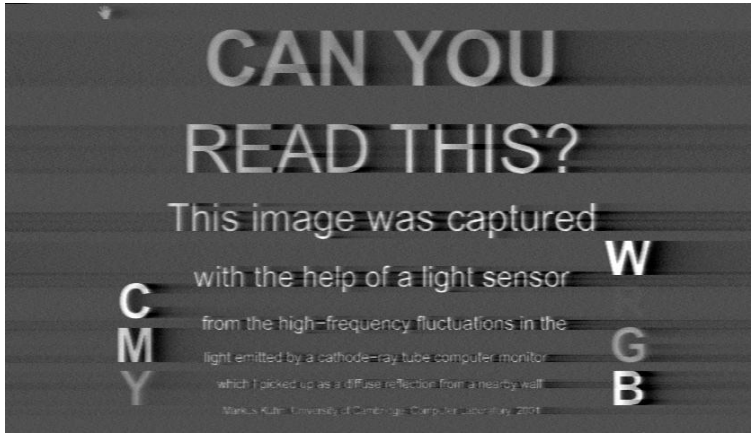


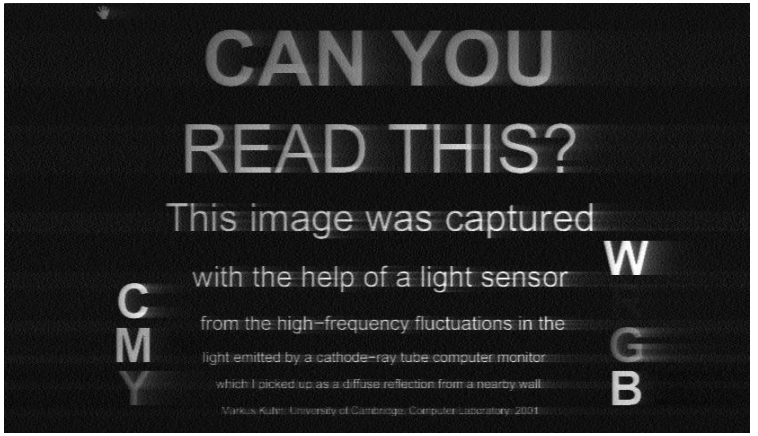
The Hamamatsu H6780-01 photosensor module used for these experiments contains a photomultiplier tube together with a high-voltage power supply.

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









Заключение.

- Существует целый ряд угроз безопасности информации, обрабатываемой средствами вычислительной техники.
- В части касающейся утечки информации по техническим каналам можно выделить следующие основные способы перехвата информации:
  - перехват побочных электромагнитных излучений, возникающих при работе СВТ;
  - перехват наводок информативных сигналов с соединительных линий ВТСС и посторонних проводников;
  - перехват наводок информативных сигналов с линий электропитания и заземления СВТ;
  - “высокочастотное облучение” СВТ;
  - внедрение в СВТ закладных устройств.
- Каждый из перечисленных способов перехвата имеет свои “сильные” и “слабые” стороны, которые необходимо чётко представлять для создания правильной модели технической разведки (оценки возможностей технической разведки) и разработки соответствующих мер противодействия.

Список используемой литературы:

- Хорев А.А. “Технические каналы утечки информации, обрабатываемой средствами вычислительной техники” http://www.analitika.info/stati2.php?page=2&full=block_article191
- Хорев А.А. “Угрозы безопасности информации” http://www.bnti.ru/showart.asp?aid=955&lvl=04.03.
- “Electromagnetic eavesdropping on computers”, Markus Kuhn, 2002-06-12, University of Cambridge, Computer Laboratory: http://www.cl.cam.ac.uk/~mgk25/publications.html
- “Compromising emanations: eavesdropping risks of computer displays”, Markus G. Kuhn, December 2003, University of Cambridge, Computer Laboratory, UCAM-CL-TR-577 ISSN 1476-2986
- www.endoacustica.com