Харьковский национальный университет радиоэлектроники

Кафедра телекоммуникационных систем

Направление подготовки: 6.170103 «Управление информационной безопасностью»

Учебная дисциплина

Основы технической защиты информации

Тема раздела: Каналы утечки информации, обрабатываемой техническими средствами передачи, обработки, хранения и отображения информации (ТСПИ), через побочные электромагнитные излучения и наводки (ПЭМИН). Методы и средства защиты информации, обрабатываемой ТСПИ, предотвращающие утечку информации через ПЭМИН.

Лекция № 9.

Общие сведения о каналах утечки информации, обрабатываемой ТСПИ, через ПЭМИН.

Учебные вопросы:

1. **История использования побочных электромагнитных излучений и наводок (ПЭМИН) для негласного съема информации.**
2. **Физические принципы возникновения ПЭМИН**

Учебный вопрос № 1. История использования побочных электромагнитных излучений и наводок (ПЭМИН) для негласного съема информации

Терминология

Побочные электромагнитные излучения (ПЭМИ) — это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами ТСПИ, специальным образом для этого не предназначенными.

Наводки от ПЭМИ – это свойство возникновения информационного сигнала в проводниках, проходящих вблизи ТСПИ, вследствие действия ПЭМИ.

Употребляемый отечественный термин – **ПЭМИН** - в зарубежной литературе имеет синонимы TEMPEST и компрометирующие излучения (compromising emanations).

TEMPEST (сокращение от Transient Electromagnetic Pulse Emanation Standard) представляет собой стандарт на переходные электромагнитные импульсные излучения (работающей радиоэлектронной аппаратуры). В обиходе термин TEMPEST, употребляемый в Соединенных Штатах используется, например, для обозначения процесса перехвата информации (TEMPEST-атаки) и т.п.

Европа и Канада в основном оперируют термином **"компрометирующие излучения".**

Исследования побочных излучений были начаты в начале 20-го века.

Самыми первыми, были работы Герберта Ядли, который разрабатывал способы выявления и перехвата скрытых радиопередач для армии США. При проведении исследований Ядли обратил внимание на присутствие побочных излучений и предположил, что они также могут нести полезную информацию.

Полномасштабные (но закрытые) исследования побочных "компрометирующих" электромагнитных излучений начались в конце 40-х - начале 50-х годов.

После окончания второй мировой войны во время прослушивания телефонных переговоров советских представительств в Берлине, американские спецслужбы обратили внимание на какой-то странный шум в виде слабых щелчков. Как выяснилось позже, это был сигнал, излучаемый электромагнитом печатающего устройства телетайпной машины, воспроизводящей открытый текст. Восстановив этот сигнал и подав его на телетайпную машину, сотрудникам ЦРУ удалось получить тот самый открытый текст.

В книге "Шпионский улов" ("Spycatcher), бывший сотрудник МИ-5 Питер Райт рассказывает о начале Tempest-атак на шифровальные машины.

В 1960-м году Великобритания вела переговоры о присоединении к Европейскому экономическому сообществу и премьер-министр был обеспокоен тем, что французский лидер де Голль выступал против этого решения.

В связи с этим служба разведки получила указание определить позицию французов на предстоящих переговорах. Попытка сломать французский дипломатический код закончилась неудачей. Однако Райт и его помощник Тони Сайл заметили, что зашифрованный трафик переносит слабый вторичный сигнал. Райт и Сайл сконструировали оборудование для его восстановления и пришли к выводу, что сигнал есть ни что иное как открытое сообщение, каким-то образом “просочившееся” сквозь шифровальную машину.

К 50-м годам относится другое открытие британских спецслужб, также описанное Питером Райтом в книге "Шпионский улов". Сотрудники британских спецслужб назвали это явление Rafter - непреднамеренное побочное излучение гетеродинов приемников, пригодное для восстановления информации.

Все исследования по TEMPEST и случаи перехвата, как правило, держались в секрете, а первое открытое описание TEMPEST-угрозы появилось в отчете шведа Кристиана Бекмана в начале 80-х.

Однако большее внимание к проблеме привлекла статья голландского ученого Вима ван Эйка, опубликованная в 1985 году.

В этой статье ("Электромагнитное излучение видеодисплейных модулей: Риск перехвата информации?") автор показал, что содержимое экрана монитора может быть восстановлено дистанционно с помощью дешевого бытового оборудования - ТВ-приемника, в котором синхронизаторы были заменены генераторами, перестраиваемыми вручную.

В феврале 1985 года ван Эйк совместно с Британской радиовещательной корпорацией провел эксперимент по "подслушиванию" с положительным результатом.. Часть полученных результатов затем была показана в программе "Мир завтра" (Tomorrow's World).

Полученные Ван Эйком результаты были позднее подтверждены Мюллером, Бернстейном и Колбергом, которые занимались разработкой различных технических приемов экранирования оборудования. Позднее, в 1987 году Смалдерс показал, что даже экранированные кабели RS-232 могут быть, в ряде случаев, прослушаны. Середину 80-х можно назвать переломным рубежом, после которого количество открытых публикаций по этой теме стало неуклонно возрастать с каждым годом. Проблема утечки информации через ПЭМИН стала исследоваться не только в закрытых военных ведомствах, но и в гражданских организациях.

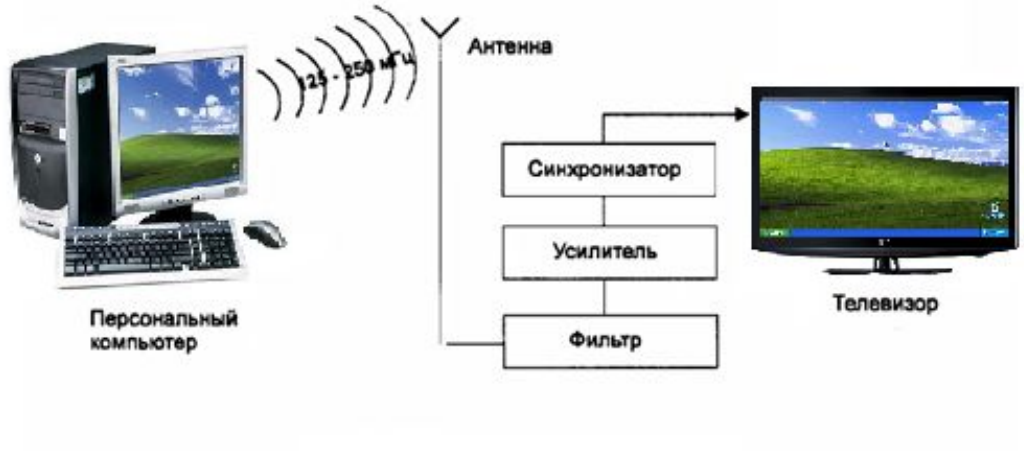
В 1994 году Комиссия по безопасности соединений представила отчет Секретарю безопасности и директору ЦРУ, названный Redefining Security ("Определение безопасности"). Несколько выдержек из этого отчета:

"Тот факт, что электронные приборы такие как, например, компьютеры, принтеры дают электромагнитные излучения, представляет собой проблему для правительства США. Злоумышленники, используя имеющиеся в наличии приборы, чаще всего мониторы, могут перехватить секретную информацию и быть в курсе событий. Для исключения этой уязвимости (уменьшения или устранения побочных излучений), правительство США обладает длинным перечнем критериев, предъявляемых к электронным приборам, который используется для классификации уже имеющегося или для проектирования нового оборудования. Альтернативным вариантом является защита некоторой зоны вокруг оборудования, обрабатывающего конфиденциальную информацию, расстояние до границ которой превышает расстояние распространения электромагнитных излучений, содержащих информацию или зон, за границами которых излучения не могут быть выявлены. Первый вариант очень дорогостоящий, так как компьютеры, соответствующие критериям TEMPEST стоят приблизительно в два раза дороже обычных. Впрочем, защита и экранирование площади также может стоить очень дорого. Пока только некоторые агентства внедрили строгие стандарты по TEMPEST, другие же или отказались или использовали различные варианты интерпретации используемого стандарта. В некоторых случаях, используется многоуровневая защита, которая не всегда адекватна фактической угрозе".

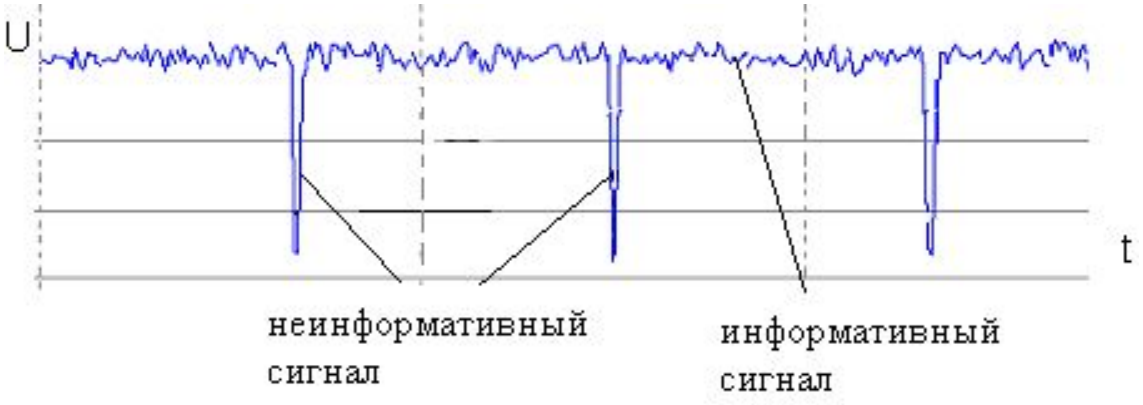
Учебный вопрос № 2. Физические принципы возникновения ПЭМИН

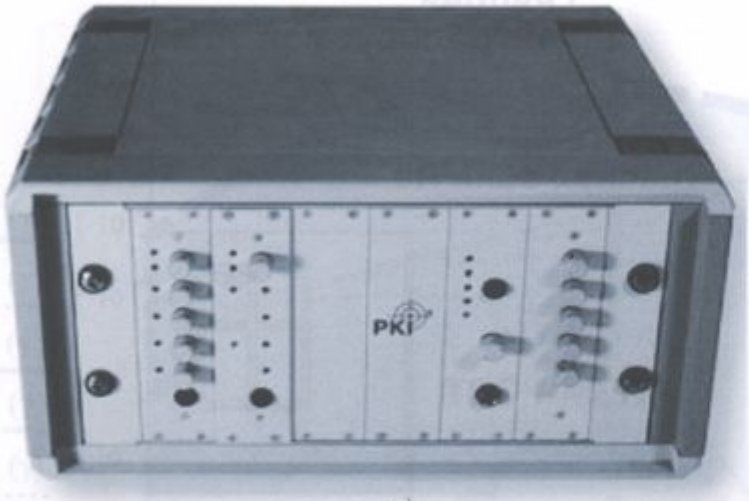
Основы технической защиты информации

Перехват информации с персонального компьютера



Сигнал изображения, выводимый на монитор





а)

б)

Рис. 3. 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)

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;

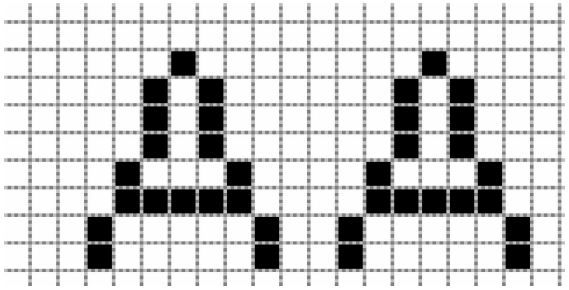
- передача данных в каналы связи;

- вывод данных на периферийные печатные устройства – принтеры, плоттеры;

- запись данных от сканера на магнитный носитель (ОЗУ).

Устройство системы отображения монитора ПЭВМ.

Экран монитора отображает информацию в виде точек (пикселей) . Количество точек зависит от установленного режима отображения. Наиболее часто используемые режимы отображения: 640 точек по горизонтали и 480 по вертикали (в данном режиме монитор работает при использовании DOS программ), 600 точек по горизонтали и 800 по вертикали, 1024 точек по горизонтали и 768 по вертикали, 1280 точек по горизонтали и 1024 по вертикали.

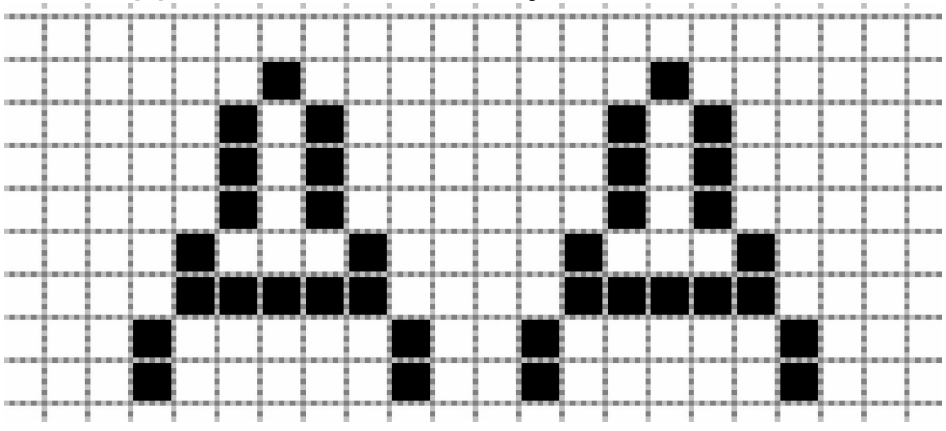


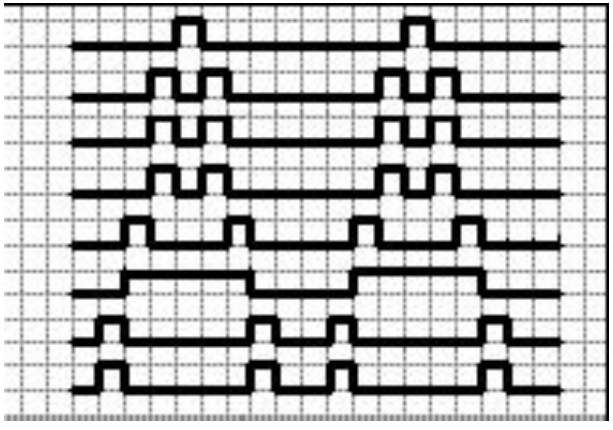
Каждая клеточка на данной картинке означает одну точку на экране. Информация о картинке передается видеокартой последовательно, точка за точкой начиная с самой верхней левой точки экрана до правой нижней.

Для экранных изображений используется цветовой режим RGB, строящийся на основе трех цветовых излучениях (красном, зеленом и синем). Цвет и его яркость передаются определенной комбинацией уровней синхронно про трем проводам R,G,B. На каждую точку тратится строго определенное время *т*. На отображение всей строки тратится время 600*т (при режиме отображения 600*800 точек). После отображения всей строки следует строчный синхроимпульс. Далее во времени отображается вторая строка, третья строка и т.д. После последней строки следует кадровый синхроимпульс.

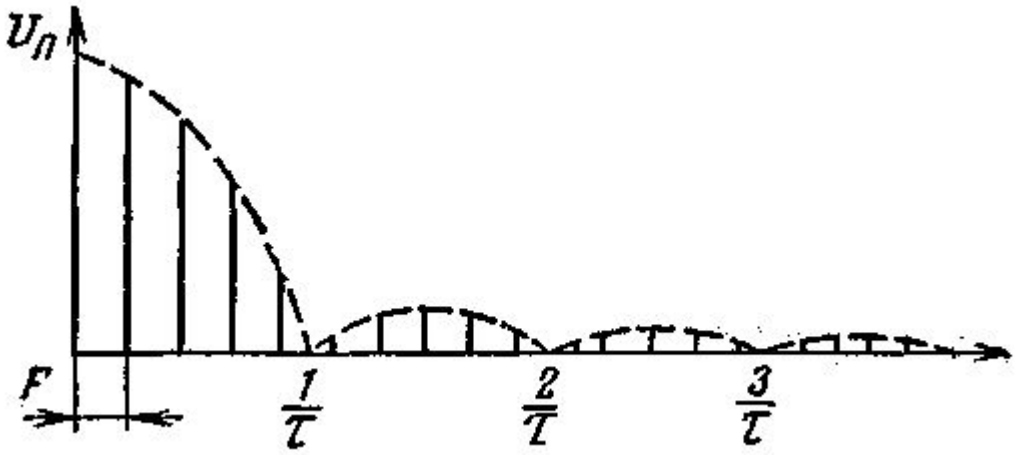
Любой текст или любая картинка передается на экран в виде цифровых импульсов разной длительности. Минимальная длительность импульса - *т* (длительность импульса, определенная временем, затраченным на отображение одной точки. Максимальная длительность – не ограничена и зависит от текста или картинки, отображаемой на экране.

Допустим, что белый цвет кодируется нулевым потенциалом линий RGB, а черный цвет – высоким уровнем потенциала линий RGB. Тогда картинка буквы «А» передаваемые в виде цифровых сигналов будет выглядеть следующим образом:





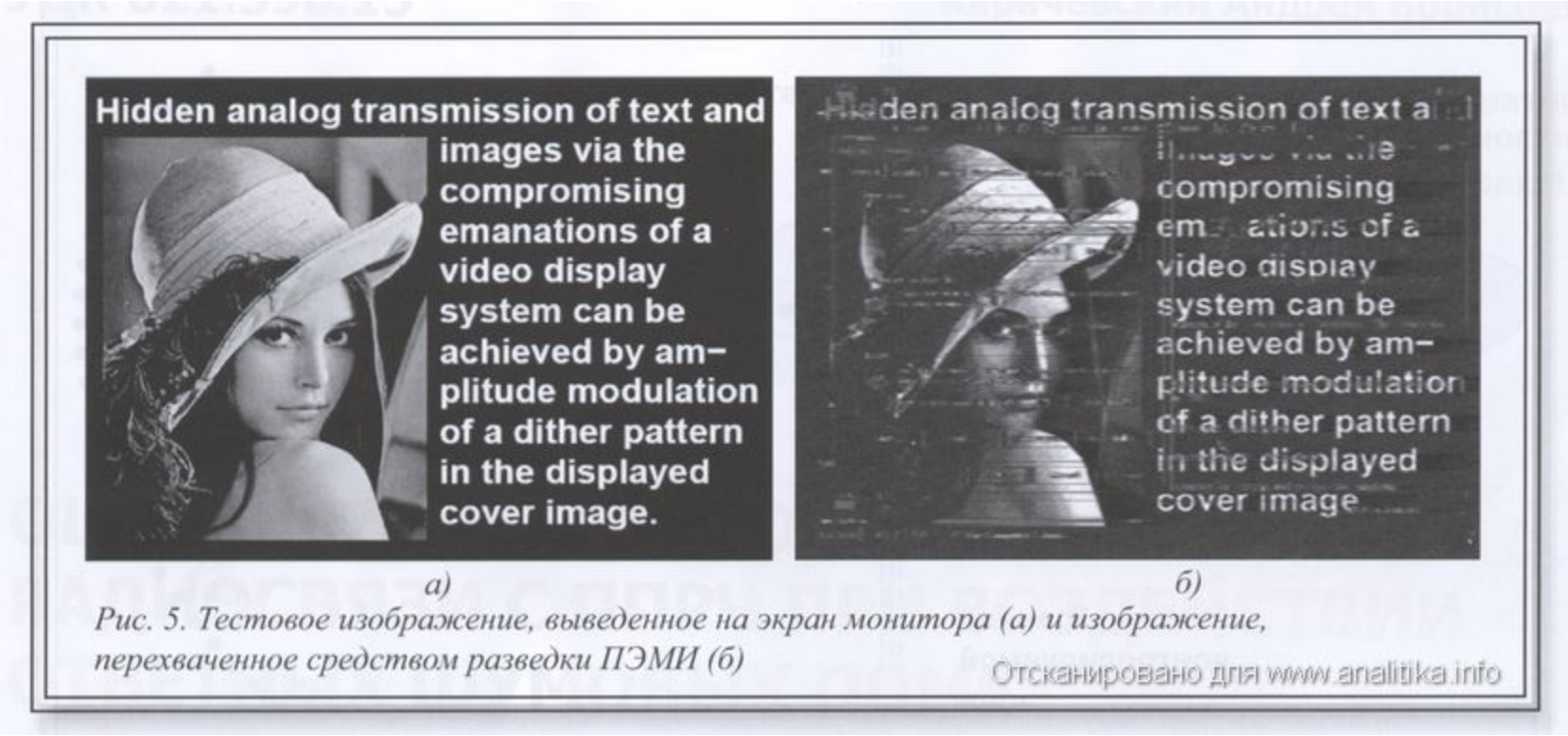
При прохождении по проводникам импульсных сигналов возникают побочные электромагнитные излучения, спектр которых представлен на рис.



Где *τ* - длительность импульса, определенная временем, затраченным на отображение одной точки.

Таким образом спектр частот сигналов излучаемых в эфир лежит от 0 до *1/τ*, далее от *1/τ* до *2/τ* и т.д. Разведывательный приемник, ориентированный на прием информации с монитора должен также иметь полосу пропускания *1/τ*. Если приемник будет иметь более узкую полосу пропускания, то сигналы с длительностью импульса равной τ приниматься и восстанавливаться не будут. Для примера монитора это означает то, что тонкие линии и буквы, нарисованные тонкими линиями перехватить нельзя. Если полоса пропускания приемника будет ниже *2/τ*, то уже линии нарисованные толщиной в две точки перехватить нельзя.

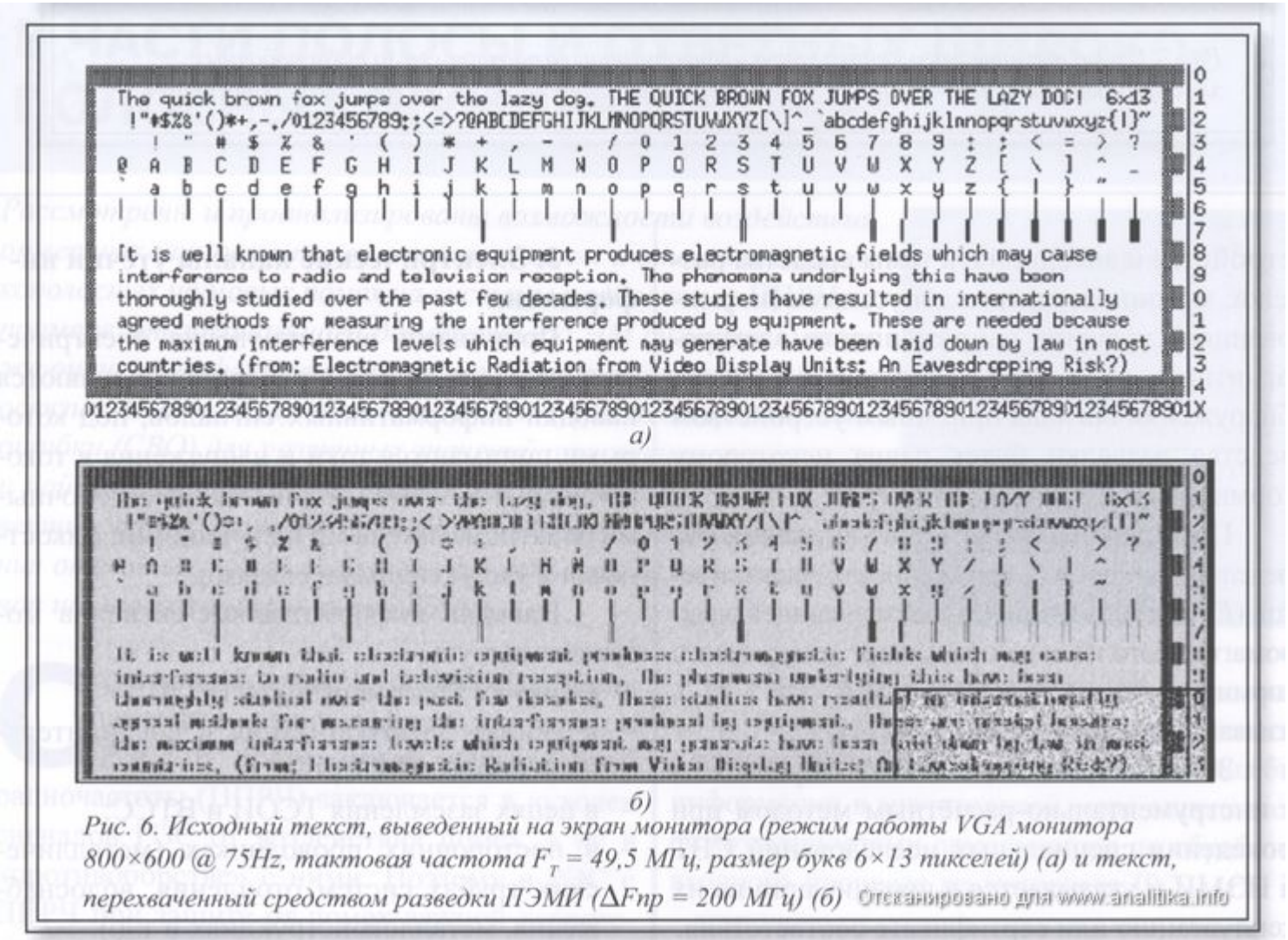
Качество перехваченного изображения значительно хуже качества изображения, выводимого на экран монитора ПЭВМ



а) *б)*

Рис. 5. Тестовое изображение, выведенное на экран монитора (а) и изображение, перехваченное средством разведки ПЭМИ (б)

Перехват текста, выводимого на экран монитора и написанного мелким шрифтом



а)

б)

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

Анализ ПЭВМ как излучающей системы

В ТСПИ (например, в ПЭВМ) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного сигнала.

Для того чтобы в радиоэфире возник радиосигнал кроме переменного электрического тока необходимо еще два условия:

1. Сигнал должен иметь определенную мощность (т.е. необходим передатчик с определенной мощностью);
2. Необходима антенная система настроенная на частоту данного переменного тока.

В качестве эквивалента передатчика в радиоцепях выступают различные генераторы, модуляторы, усилители или просто выходы цифровых микросхем.

В качестве антенных систем выступают отрезки проводников по которым распространяется радиосигнал, внутренние жгуты проводов связывающие между собой отдельные платы, разъемы и элементы конструкции, и, наконец, внешние кабели соединяющие отдельные устройства.

Влияние антенны на мощность ПЭМИ

Качество антенны можно оценить по длине излучающего кабеля. Чем ближе длина прямолинейного отрезка кабеля к длине волны (или к кратной ей величине), тем лучше качество излучающей антенной системы. Если излучающая антенна представляет собой диполь, то в идеальном случае его размер должен быть равен 1/2 длины волны. Если антенной является просто отрезок проводника (т.е. антенну можно рассматривать как штырь), то для оптимального излучения его длина должна бать кратна длине волны.

На практике длина излучающей антенной практически никогда не согласована с первой гармоникой, так как самые длинные кабели – около 1.5 м (принтер и монитор) начинают эффективно работать на частотах выше 100 МГц, а внутренние проводники исходя из их длины на частотах выше 400-500 МГц. Поэтому, реальная антенная система может быть согласована с длиной волны например, 10-й или более высокой гармоники. В этом случае, вклад качества антенной системы на частоте 10-й гармоники может быть значительнее затухания сигнала 10-й гармоники и сигнал (напряженность поля) на частоте 10-й гармоники может иметь амплитуду сравнимую или даже выше, чем амплитуда 1-й гармоники. На практике это выглядит следующим образом: сначала амплитуды сигналов уменьшаются по мере увеличения номера гармоники, а затем, на частоте 400-500 МГц (т.е. 10-40 гармоника для монитора) неожиданно может быть зафиксирован резкий всплеск амплитуды сигнала ПЭМИН.

Влияние антенны на мощность ПЭМИ

Излучающие свойства антенны зависят не только от ее длины, но и от положения ее в пространстве. Более того, проводник длиной 1 метр как антенна согласован с частотой 300МГц только в том случае, если этот проводник вытянут в прямолинейный отрезок.

Если проводник каким-то образом скручен, зажгутован или проложен по криволинейной траектории, то его резонансная частота как правило увеличивается. Поэтому, излучающие свойства ПЭВМ (ТС) зависят от расположения его блоков и узлов.

ПРИМЕР

Для примера возьмем ставший уже хрестоматийным пример монитора 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.

Пример измерения уровня ПЭМИ мониторов ЗАО «РАМЭК-ВС»

Так, при формировании одного из заказов в 2004 г. уровни ПЭМИ от электронно-лучевого монитора не удовлетворяли требованиям заказчика (кривая 1 на рисунке), в связи с чем он был заменен жидкокристаллическим монитором с низким уровнем излучения (кривая 2). В 2005 г. тот же заказчик решил приобрести еще одну партию аналогичных СВТ. Однако оказалось, что жидкокристаллические мониторы той же модели и того же производителя дают уже другой уровень ПЭМИ (кривая 3).

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.

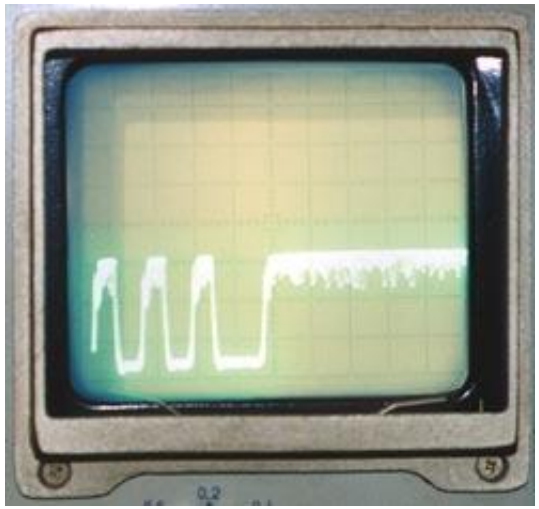


Рис. 1. Последовательный код знака = на экране осциллографа, подключенного к коротковолновому приемнику

Исследование уровней излучения, создаваемых компьютерами в различных серийно выпускаемых корпусах.

Результаты измерений уровня электрической (рис.2) и магнитной (рис.3) составляющих показал, что у компьютеров с различными серийно выпускаемыми корпусами системных блоков мощность побочных излучений от клавиатуры может отличаться более чем в 100 раз.

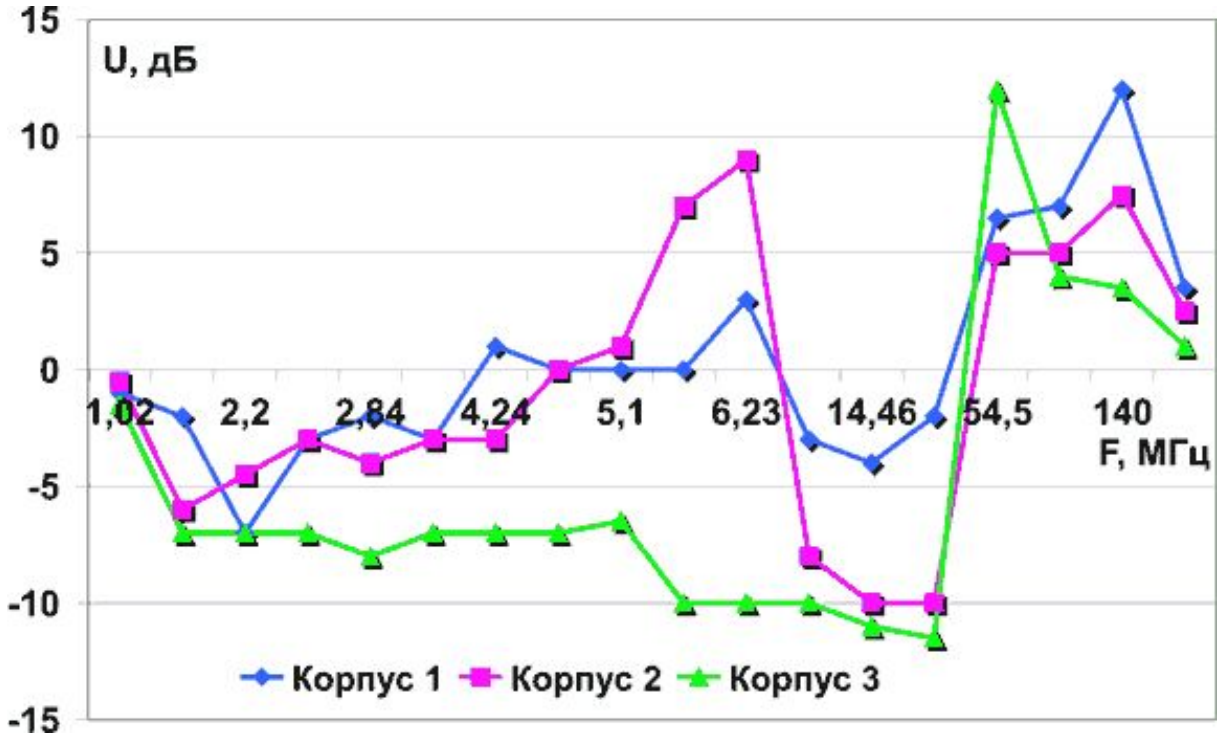


Рис.2. Уровень электрической составляющей ЭМП излучения клавиатуры

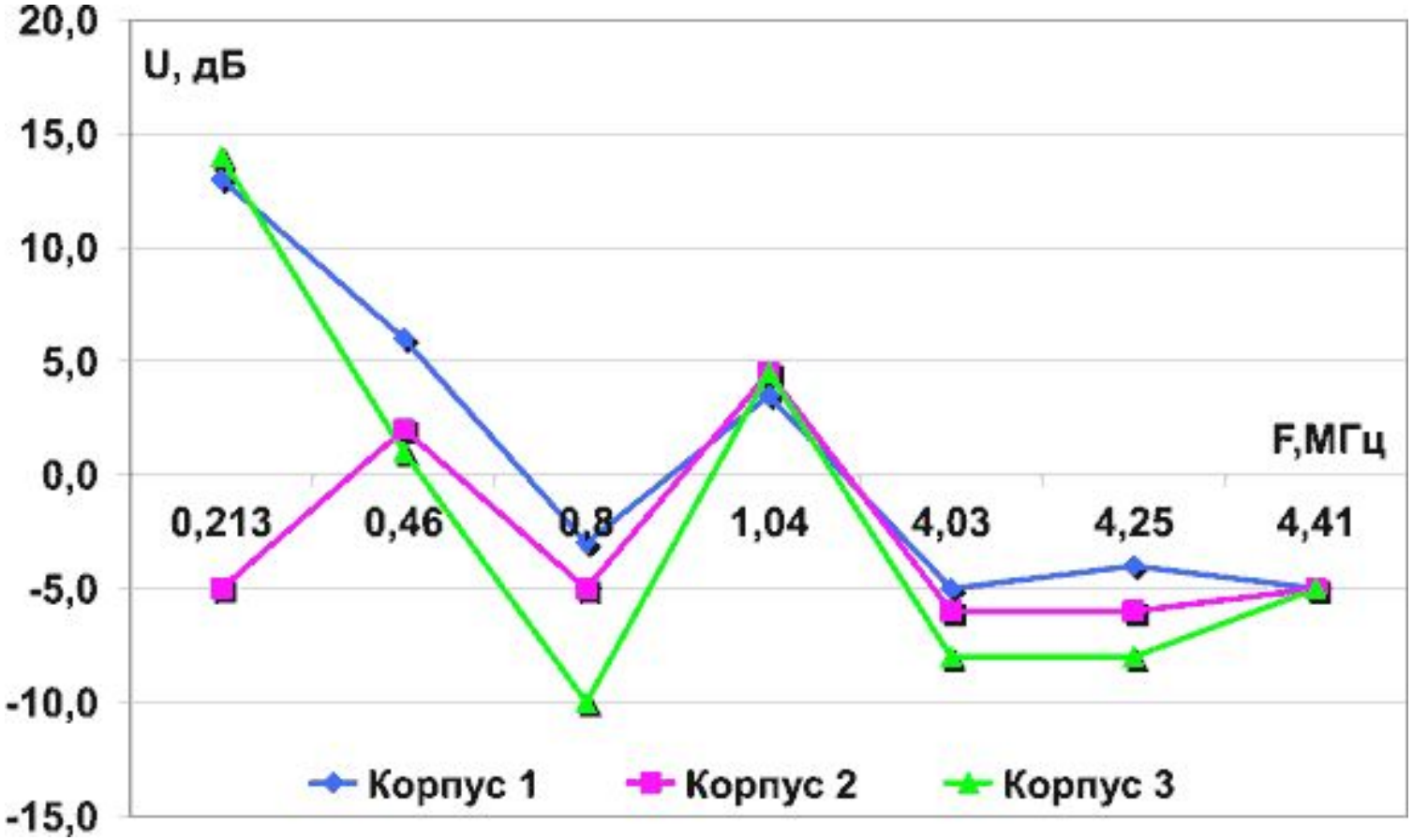


Рис.3. Уровень магнитной составляющей ЭМП излучения клавиатуры

Результаты исследований показали, что современные корпуса позволяют значительно ослабить излучения элементов компьютера.

Побочные излучения кабельной системы

Кабельная система не содержит активных или нелинейных элементов, поэтому сама по себе она не может быть источником побочных излучений. Однако кабельная система связывает между собой все элементы компьютерной сети. По ней передаются сетевые данные, но вместе с этим она является также приемником всех наводок и **средой для переноса побочных электромагнитных излучений**

Поэтому различают:

1. Побочное излучение, вызванное передаваемыми по данной линии сигналами (трафиком локальной сети);

2. Прием и последующее переизлучение побочных излучений от расположенных вблизи других линий и устройств;

3. Излучение кабельной системой побочных колебаний от элементов сетевого активного оборудования и компьютеров, к которым подключен кабель.

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.

Контрольные вопросы:

1. Режимы обработки информации средствами вычислительной техники при которых возникают побочные электромагнитные излучения.
2. Провести анализ ПЭВМ как излучающей системы.
3. Пояснить особенности функционирования монитора ПЭВМ, как излучающей системы.
4. Пояснить особенности функционирования клавиатуры ПЭВМ, как излучающей системы.
5. Пояснить, что такое информативные ПЭМИ и неинформативные ПЭМИ.