3 Забезпечення комп'ютерної безпеки державних, банківських та інших інформаційних систем

УДК 621.396.2

УМЕНЬШЕНИЕ ИНФОРМАТИВНОГО ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПОСЛЕДОВАТЕЛЬНЫМ СПОСОБОМ

Игорь Курдин, Виктор Найденко, Михаил Прокофьев
Национальный технический университет Украины «КПИ», НИЦ «Тезис»

Аннотация: **Рассмотрены проблемы уменьшения побочного электромагнитного излучения компьютера и периферийных блоков. Проанализированы зарубежные статьи о возможности диагностики, приема и восстановления информативного ПЭМИ компьютеров. Рассмотрен способ уменьшения уровня информативного ПЭМИ путем увеличения длительности переходных процессов при передаче информации последовательным способом.**

Summary: **The problems of diminution of compromising emanation and EMI of the computer and other electronic equipment are surveyed. The public descriptions about an opportunity of diagnostics and reconstructing compromising emanation of computers are analyzed. The method of diminution of a level informative EMI is surveyed by magnification of duration of transient processes at an information transfer by a sequential method.**

Ключевые слова: **Защита информации, побочное электромагнитное излучение, шрифты, EMI, compromising emanation.**

Побочное электромагнитное излучение (ПЭМИ) является одним из возможных каналов утечки информации при ее обработке на компьютере. В настоящее время много внимания уделяется активной (генераторы шума, постановщики помех) и пассивной защите (полное или частичное экранирование составных блоков компьютера и его периферии) [1]. Считается, что наиболее эффективным, экологически чистым и повышающим уровень биологической защиты оператора от вредного воздействия ПЭМИ является пассивный метод. Но, как пассивный, так и активный метод предполагают борьбу со следствием – с уже созданными средствами вычислительной техники ПЭМИ. Логичным является стремление уменьшить уровень ПЭМИ в момент его возникновения.

Известны зарубежные источники, в которых проводится анализ возможности приема ПЭМИ компьютера, возникающего вследствие переходных процессов при передаче (обработке) информации последовательным способом с последующим восстановлением. Рассмотрим некоторые из них.

1. В 1988 году Peter Smulders [2] исследовал принципы приема и возможность восстановления ПЭМИ от сигнального кабеля, подключенного к порту RS-232, и на практике подтвердил возможность приема и восстановления передаваемой информации. В экспериментах в качестве приемника он использовал обычный приемник коротковолнового диапазона.

Подключенные к сигнальному кабелю элементы формируют цепи, состоящие из индуктивности кабеля и емкости между устройством и землей. Эти цепи возбуждаются высокочастотными составляющими, возникающими при переходных процессах во время передачи данных, и как результат, элементы схем излучают ПЭМИ, которое содержит временную информацию.

Были приведены осциллограммы (рис. 1) исходного и принятого коротковолновым приемником сигналов на расстоянии 7 метров. Частота приема – 16 МГц, вид демодуляции – АМ. Момент перехода от логического «0» к логической «1» в исходной осциллограмме характеризуется появлением информативного ПЭМИ, которое было принято, продетектировано и подано на второй вход осциллографа для сравнения.

При использовании бытового приемника FM диапазона (ЧМ-детектор) при приеме на частоте 98 МГц принятый сигнал имел практически такой же вид, как и исходный (рис. 2).

2. В 1985 году Wim van Eck [3] исследовал возможность приема и восстановления информации, выводимой на экран монитора. Он создал макет устройства и практически подтвердил работоспособность устройства. Макет был изготовлен из обычного телевизора. Для дальнейших исследований и измерений использовался анализатор HP8586A (30 – 300 МГц), осциллограф и биконическая антенна, установленная на расстоянии 1 метр. Измерения проводились по двум стандартным методикам (NACSIM 5100A, AMSG 720B). На рис 3. показаны полученные осциллограммы: вверху – осциллограмма исходного информационного сигнала, подаваемого от системного блока по сигнальному кабелю на монитор, ниже – осциллограмма

принятого сигнала на выходе промежуточной частоты телевизионного приемника, внизу – осциллограмма на выходе детектора телевизионного приемника.

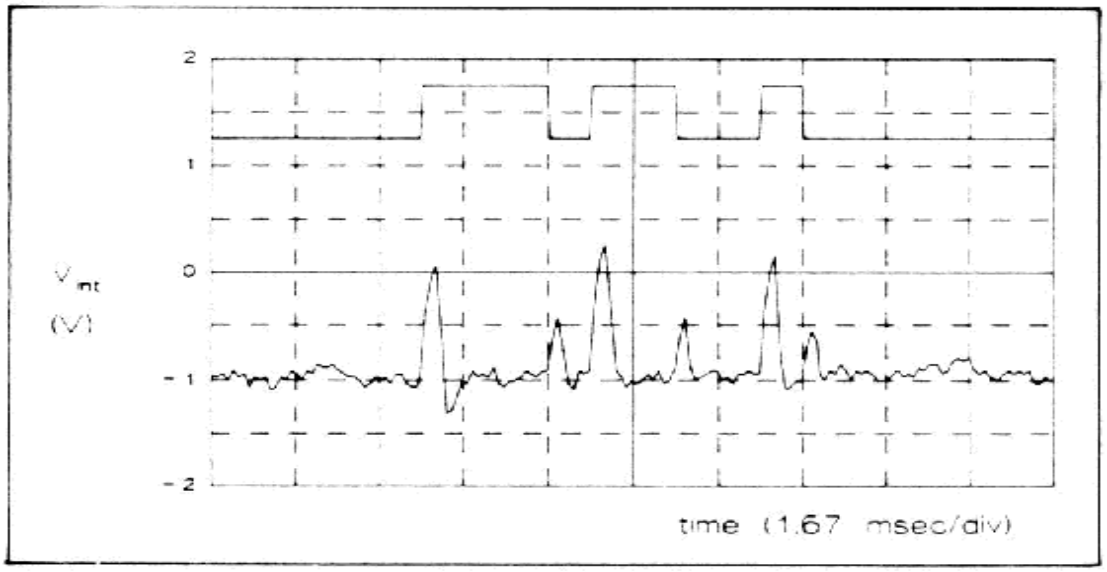

Рисунок 1 – Исходный и принятый информационный сигнал
на расстоянии 7 метров (частота приема - 16 Мгц, вид демодуляции – АМ)

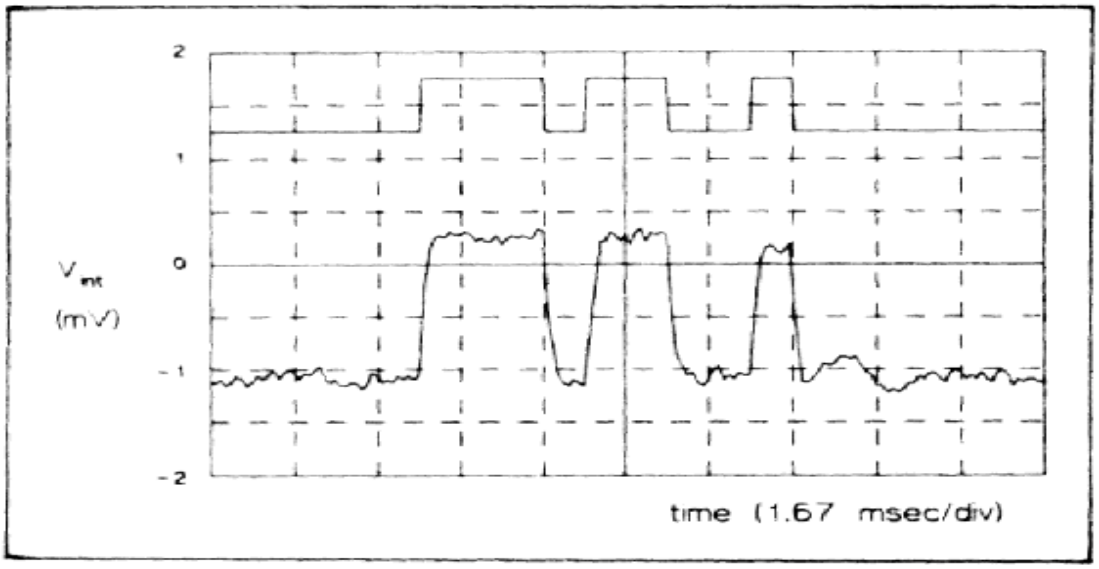

Рисунок 2 – Исходный и принятый информационный сигнал
на расстоянии 7 метров (частота приема - 98 МГц, вид демодуляции – ЧМ)

3. В 1998 году Markus G. Kuhn и Ross J. Anderson [4] исследовали информативное ПЭМИ от монитора компьютера и определили, при каких условиях излучение максимально, а при каких – минимально.

Предварительно они изучили коммерческий спрос на защищенные компьютеры и пришли к выводу, что стоимость полностью экранированных компьютерных средств была в 3, иногда в 4 раза выше, чем обычных компьютеров той же конфигурации. Основными потребителями защищенных (экранированных) компьютеров были оборонные ведомства и некоторые государственные учреждения. Представители среднего и крупного бизнеса потребителями были редко, хотя спрос на средства защиты обрабатываемой на компьютере информации был достаточно высоким. Поэтому исследования были ориентированы на

разработку недорогих средств защиты, направленных на массового потребителя, которые в то же время значительно уменьшили бы уровень информативного ПЭМИ.

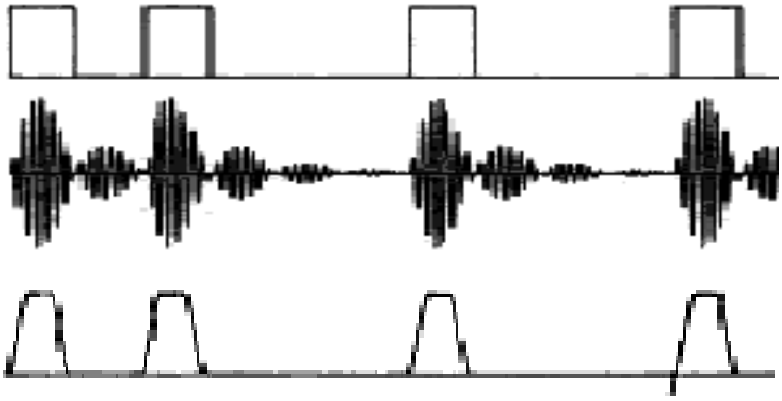

Рисунок 3 – Осциллограммы исходного сигнала (вверху), на выходе промежуточной частоты приемника (посредине), на выходе детектора приемника (внизу)

Для выявления и исследований свойств информативного ПЭМИ был взят обычный коротковолновый приемник со встроенной антенной и сгенерировано специальное изображение на мониторе (на видео вход монитора подавался меандр с частотой тона в диапазоне слышимых частот). Изменение прослушиваемого приемником тона в соответствии с изменением вида изображения, выводимого на монитор, является доказательством наличия в общем ПЭМИ информативной его части. В результате, дальность приема обычным коротковолновым приемником со встроенной антенной при косвенной оценке составила несколько комнат. Было замечено, что уверенный прием на больших расстояниях был тогда, когда антенна приемника подводилась близко к линиям электропитания. Такой эффект является логичным, так как подключенные к компьютеру длинные линии электропитания являются более эффективными антеннами, чем короткие (не более 1 метра) элементы самого компьютера, являющиеся эффективными в диапазоне выше 30 МГц.

Для экспериментального определения участка спектра изображения, выводимого на экран, имеющего наибольший удельный вес в информативном ПЭМИ, было применено тестовое изображение, сгенерированное по функции $\cos(x^2 + y^2)$. Начало координатной системы находится в центре экрана (рис. 4, вверху). В качестве приемника тестового изображения был использован приемник ESL-400, производитель DataSafe Ltd. Cheltenham, Великобритания. Приемник имеет следующие основные параметры – диапазон 20 – 860 МГЦ, полоса пропускания 8 МГц, чувствительность от 60 мкВ на частоте 20 МГц до 5 мкВ на частоте 860 МГц. Синхронизация – ручная. Антенна – короткий вибратор.

Принятое изображение (рис. 4, внизу) на мониторе приемника выглядит в виде двух столбцов. На принятом изображении видно, что не все части сигнала одинаково эффективно излучают.

В результате было установлено, что наибольший удельный вес в излучении информативного ПЭМИ имели высокочастотные составляющие спектра изображения, выводимого на экран монитора. Логичным было предположение, что для уменьшения уровня информативного ПЭМИ необходимо уменьшить уровень высокочастотных составляющих спектра изображения, выводимого на экран монитора.

Для подтверждения этого предположения были созданы специальные шрифты (патент – UK № 9801745.2), при выводе которых на экран уровень высокочастотных составляющих спектра изображения становился значительно ниже по сравнению со спектром изображения при применении обычных шрифтов.

Уровень высокочастотных составляющих обратно пропорционален времени переходных процессов, возникающих при выводе шрифтов на экран видеомонитора. Поэтому шрифты разработаны таким образом, чтобы с одной стороны время перехода от логической «1» к логическому «0» и наоборот были максимально длинными. С другой стороны – во-первых, учитывались требования по времени срабатывания цифровых микросхем, формирующих шрифты и, во-вторых, учитывался визуально заметный побочный эффект – появление расплывчатости букв при увеличении длительности переходных процессов. Длительность перехода подбиралась экспериментально.

При рассмотрении с близкого расстояния расплывчатость символов заметна (рис. 5, справа, вверху). Из-за того, что человеческий глаз играет роль сглаживающего фильтра, созданная расплывчатость в результате фильтрования на значительном расстоянии практически не видна (рис. 5, справа, внизу).

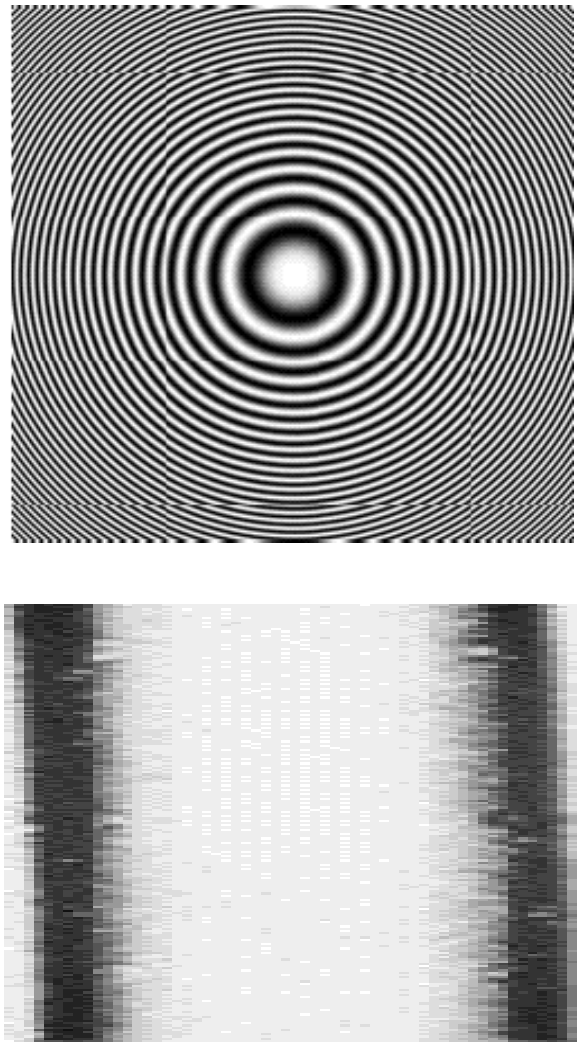

Рисунок 4 – Вверху тестовое изображение, сгенерированное по закону функции cos ($x^2 + y^2$); начало координатной системы находится в центре экрана; внизу – принятое изображение

На рис. 5. показаны фрагменты применения обычных и созданных специальных шрифтов. Слева вверху – фрагмент исходного шрифта на мониторе при рассмотрении с близкого расстояния, справа вверху – фрагмент разработанного шрифта при рассмотрении с близкого расстояния, слева внизу – фото фрагмента исходного текста на мониторе при рассмотрении с обычного расстояния, справа внизу – фото разработанного шрифта при рассмотрении с обычного расстояния. Фильтрованный текст в увеличенном представлении имеет довольно неприятный для глаза вид, но потеря в текстовом качестве почти незаметна для пользователя, смотрящего на монитор с обычного расстояния (нижняя половина рис. 5).

Изначально недорогое техническое решение в защите передаваемой последовательным кодом информации будет оптимальным и массовым решением защиты информации в аспекте уменьшения уровня информативного ПЭМИ. Область возможного применения – некоторые государственные органы, банки, крупные и средние компании, где рекомендовано использовать зональную модель, в которой компьютеры с конфиденциальной информацией не ограждены, но локализованы в отдельных комнатах и находятся далеко от помещений общего доступа.

Уменьшение уровня информативного ПЭМИ за счет увеличения длительности переходных процессов при передаче данных последовательным способом может использоваться не только в целях защиты информации, обрабатываемой на компьютере (передача данных с клавиатуры в системный блок компьютера, передача данных в локальных компьютерных сетях, передача информации на видеомонитор, считывание и запись информации на дисковод, передача информации на принтер и т. д.), но и при вводе персональных

данных и обработки информации в банкоматах, в процессе считывания информации с магнитных карточек, в системах разграничения доступа и т. д.

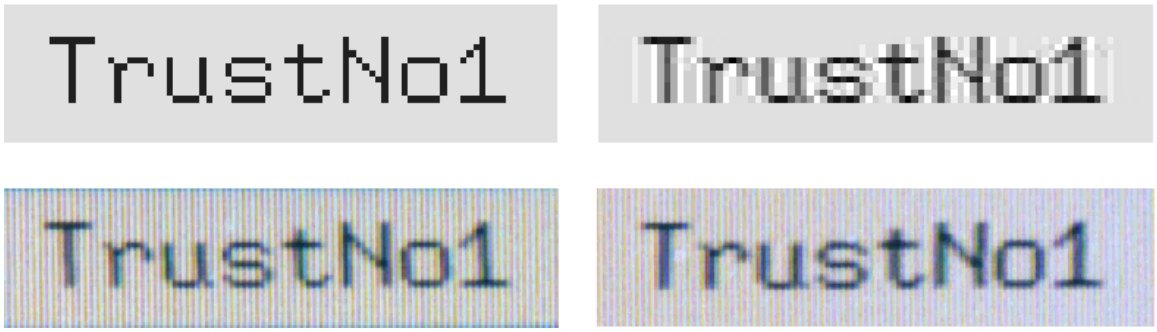

Рисунок 5

Основное достоинство – это относительная дешевизна и универсальность (применимо к любому уже установленному и работающему обычному компьютеру).

Оценить эффективность предложенного метода довольно сложно, хотя изначально очевидно уменьшение уровня информативного ПЭМИ при малых затратах.

Литература: 1. Збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформаціїї в Україні"- Київ, 2000. 2. Peter Smulders: The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security vol 9, pp 53-58, 1990. 3. W. Van Eck, Electromagnetic radiation from video display units. Computers&.Security vol. 4, pp. 269-286, 1985. 4. Markus G. Kuhn u Ross J. Anderson «Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations» - University of Cambridge, 1998.

УДК 681.3.067:336.71

ОСОБЕННОСТИ ЗАШИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

Светлана Шаповалова, Оксана Галепа, Владимир Кальганов
Национальный технический университет Украины "КПИ"

Аннотация: **Приводится обзор описанных в наиболее общей форме средств защиты информации в банках.**

Summary: **In this article was described the methods of information's protection in banks in the most general form.**

Ключевые слова: **Несанкционированный доступ к информации, защита информации в банках.**

I Задача определения необходимых мер для защиты банковской информации

Была поставлена задача определения в наиболее общей форме мер защиты информации в автоматизированных банковских системах (АБС). Задача рассматривается с точки зрения специалистов компьютерной безопасности банка, использующих готовые решения по аппаратному и программному обеспечению (ПО). Обзор охватывает основные аспекты планирования комплексной защиты, которые должны учитываться специалистами до покупки оборудования и ПО.

Под угрозой безопасности информации будем понимать несанкционированный доступ к данным на любом уровне без анализа действий нарушителя и возможных последствий.

Ограничим рассмотрение мер по защите информации следующими допущениями:

1. Будем считать, что безопасности не угрожают системные администраторы. Угроза исходит только извне или со стороны рядового пользователя.

2. Будем рассматривать работу АБС только в обычном рабочем режиме. Оставим без внимания такие аспекты проблемы, как обеспечение безопасности информации при проведении ремонтно-профилактических работ и при аварийных ситуациях.

3. Отнесем проблему заражения системы вирусами к последствиям несанкционированного доступа и вынесем за рамки нашего исследования.