УДК 004.4.056.53

Пархоменко И.И., Язиванова М.В.

МЕТОДЫ ПРОТИВОСТОЯНИЯ ТЕХНОЛОГИИ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ SOFT TEMPEST

В статье рассматривается канал утечки информации через побочные электромагнитный излучения. Спектр частот ПЭМИ ПК. Рассматривается дисплей, как самая опасная составляющая ПК из-за сильного электромагнитного излучения и как компонент к которому применяется технология Soft Tempest. В тоже время подробно описывается способ применения технологии Soft Tempest. И в конце статьи определяются самые оптимальные методы защиты от утечки информации из-за применения технологии Soft Tempest.

Ключевые слова: Soft Tempest, ПЭМИН, TEMPEST-шрифты, монитор ПК, защита информации.

Вступление. Как известно, любое радиоэлектронное устройство в процессе своего функционирования образует побочные излучения и наводки, в том числе и информативные (то есть содержащие обрабатываемую информацию). Эти излучения и наводки в отечественной литературе сокращенно именуются – ПЭМИН. Данный термин в иностранной литературе имеет синонимы «TEMPEST» и «compromising emanations» (компрометирующие излучения).

Постановка задачи и ее актуальность. Технология Soft Tempest — технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств. Разработали эту технологияю сотрудники компьютерной лаборатории Кембриджского университета Маркус Кун (Markus G.Kuhn) и Росс Андерсон (Ross J.Anderson). Особенностью технологии Soft Tempest является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Цель моей работы является определения методов борьбы с утечкой данных через эту технологию.

Канал ПЭМИН является единственным способом для злоумышленника получить конфиденциальные данные, не проникая в помещение или контактируя с людьми, и при этом быть незамеченным.

Спектр частот ПЭМИ ПК представлен колебаниями в достаточно широком диапазоне: от единиц мегагерц до нескольких гигагерц. Диаграмма направленности побочного электромагнитного излучения ПК не имеет ярко выраженного максимума, что неудивительно: взаиморасположение составных частей ПК (монитор, системный блок, проводники, соединяющие отдельные модули) отличается большим количеством вариантов.

Наиболее опасные сигналы (потенциально-информативными ПЭМИ) создает элементы ПК, в особенности в пластмассовых неметаллизированных корпусах. Ориентировочные дальности обнаружения радиоизлучений широко распространенных ПЭМИ зарубежного производства приведены в табл. 1.

Из таблицы можно сделать вывод, что самым мощными источниками электромагнитного излучения являются дисплей.

Изображение на экране дисплея формируется в основном так же, как и ТВ-приемнике — оно состоит из светящихся точек на строках. Видеосигнал является цифровым: сигнал логическая единица создает световую точку, а логический нуль препятствует ее появлению. Однако в цепях дисплея присутствует не только видеосигнал, но и тактовые синхроимпульсы.

Таблица 1

Наиболее опасные сигналы создаваемые элементами ПК

ПЭМИ	Дальность обнаружения полей, м электромагнитного	электрического
Системный блок	2 – 40	1 - 30

Дисплей	25 – 120	10 - 55
Клавиатура	15 – 50	15 - 30
Печатающее устройство	5 – 35	10 -80

Поскольку последние повторяются, то энергетический спектр видеосигнала содержит гармоники, интенсивность которых убывает с ростом частоты. Источником излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения электронным лучом кинескопа. В отличие от других сигналов, существующих в дисплее, видеосигнал усиливается до нескольких десятков вольт для подачи на электронно-лучевую трубку (ЭЛТ).

Что же касается безопасности TFT мониторов, то она не намного лучше, чем у CRT мониторов. По крайней мере, сейчас можно встретить CRT монитор с уровнем излучений не выше, чем у многих TFT мониторов. Кроме того, сигналы, необходимые для получения изображения, формируются в видеокарте и по достаточно длинному (в радиотехническом смысле) кабелю подаются на монитор. Поэтому сигналы монитора можно перехватить и вообще без монитора. Был бы только кабель. К тому благодаря своей периодической природе, видеосигнал легко выделяется из других периодическим усреднением. [3]

Вплотную к вопросу скрытой передачи информации путем излучения монитора примыкает вопрос визуального наблюдения за экраном монитора. Если к вопросу сохранности секретных сведений относятся сколь-нибудь внимательно, то монитор будет установлен таким образом, чтобы его нельзя было рассмотреть через окно. Недоступен монитор будет и для обзора случайными посетителями. Однако световой поток экрана монитора отражается от стен, и этот отраженный световой поток может быть перехвачен. Современная техника позволяет восстановить изображение на мониторе, принятое после многократных отражений его от стен и всех предметов.

Такой канал может эксплуатироваться длительное время. Единственным недостатком ПЭМИН является то, что злоумышленнику нужно ждать, когда пользователь обратится к нужной ему информации, и только тогда из полученных ПЭМИН можно выделить необходимую информацию.

Ожидания обращения к нужным данным пользователем может продолжаться долго, это могут быть дни, недели, месяцы. Ученые Кембриджского университета (M. Kuhn и R. Anderson) попытались заставить компьютер передавать необходимые данные практически в любой какой момент, то есть целью было исследовать, можно ли управлять процессом генерирования информативных излучений. Для этого им необходимо было создать программную закладку которая осуществляла поиск необходимых данных на компьютере и с помощью модуляции изображения монитора передавала ее каналам ПЭМИН. Данная технология получила название Soft TEMPEST.

Технология реализации атаки с использованием программной ПЭМИН на примере компьютера состоит в следующем: в "компьютер-жертву" любым из доступных методов злоумышленником интегрируется специальная программа. Задачей программы является поиск необходимой информации (необязательно на жестком диске) и путем обращения к различным аппаратных средств компьютера создать побочные излучения, которые будут промоделированы информативными битами. Перехватывая эти излучения и выделяя информативную составляющую злоумышленник получает желанную информацию.

Особенностью технологии Soft Tempest является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Действительно, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН нет, а обнаружить такое излучение в общем широкополосном спектре

(более 1000 МГц) паразитных излучений ПК без знания параметров полезного сигнала весьма проблематично.

Основная опасность технологии Soft Tempest заключается в скрытности работы программы-вируса. Такая программа в отличие от большинства вирусов не портит данные, не нарушает работу ПК, не производит несанкционированную рассылку по сети, а значит, долгое время не обнаруживается пользователем и администратором сети. Поэтому, если вирусы, использующие Интернет для передачи данных, проявляют себя практически мгновенно, и на них быстро находится противоядие в виде антивирусных программ, то вирусы использующие ПЭМИН для передачи данных, могут работать годами, не обнаруживая себя. [1]

В действительности ПЭМИН-сигнал - это грубо говоря амплитуда производной видеосигнала. С текстом это обычно не составляет проблемы, поскольку знаки (в большинстве языков) идентифицируются по их вертикальным компонентам; но это мешает приему экранных изображений типа фотографий, которые не удается легко восстанавливать лишь по четким вертикальным краям.

Человеческий глаз менее чувствителен к высоким, нежели к низким частотам колебаний. "Дрожание" (dithering) - это техника, использующая данное свойство глаза для увеличения цветовых оттенков на дисплеях с небольшим размером таблицы цветности. На современных мониторах с высоким разрешением пользователь не может легко отличить средне-серый цвет от паттерна шахматной доски из черных и белых пиксел, особенно когда расстояние между пикселами меньше диаметра фокуса электронного луча. Для перехватчика же, с другой стороны, высокочастотный черно-белый паттерн порождает максимально возможный по силе сигнал, в то время как постоянный цвет приводит к наислабейшему сигналу.

Можно использовать эту разницу в спектральной чувствительности пользователя и перехватчика для того, чтобы они видели различную информацию.

В то время как компьютерный монитор явно высвечивает здесь большими буквами "Оксфорд", перехватчик вместо этого видит на своем экране "Кембридж". На Рис.1 изображено увеличение поля пиксел вокруг букв "Ox", излучающих как "Ca". В то время как "Oxford" нарисован розовым вместо серого путем простого выключения зеленой компоненты, "Cambridge" вставлен в картинку наращиванием амплитуды дрожания.

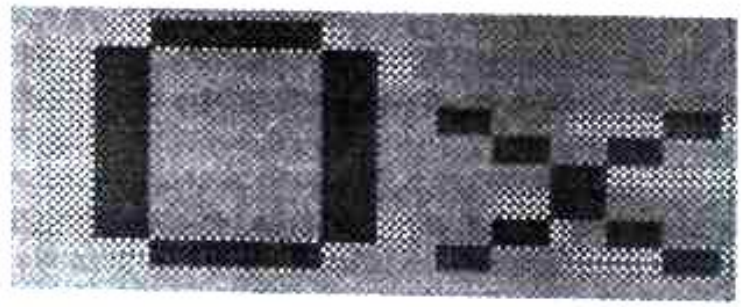

Рис. 1. Увеличение фрагмента экрана, где пользователь читает "Ox", а на экране перехватчика этот же участок читается как "Ca".

Изменение амплитуда дрожания должно быть сглаженным, чтобы не возбуждать очень чувствительные детекторы в сетчатке человеческого глаза. Для того, чтобы изменение было невидимым, надо учитывать несколько физических эффектов мониторов. Значение цветового компонента, выбираемого дисплейной программой, обычно линейно отображается в напряжение видеовхода, подаваемого на монитор. Но соотношение между

видеонапряжением V и светимостью L экрана нелинейно и может быть аппроксимировано как

$$L = const*V*y,$$

где y - зависящая от аппаратуры экспонента, обычно имеющая значение в пределах 1.5-3, в зависимости от конструкции катодно-лучевой трубки. Программисту следует помнить, что общая светимость двух цветовых дрожащих паттернов зависит от среднего арифметического их светимостей, а не от напряжений.[5]

Способы предотвращения утечки информации через Soft TEMPEST обозначены на рисунке 2:

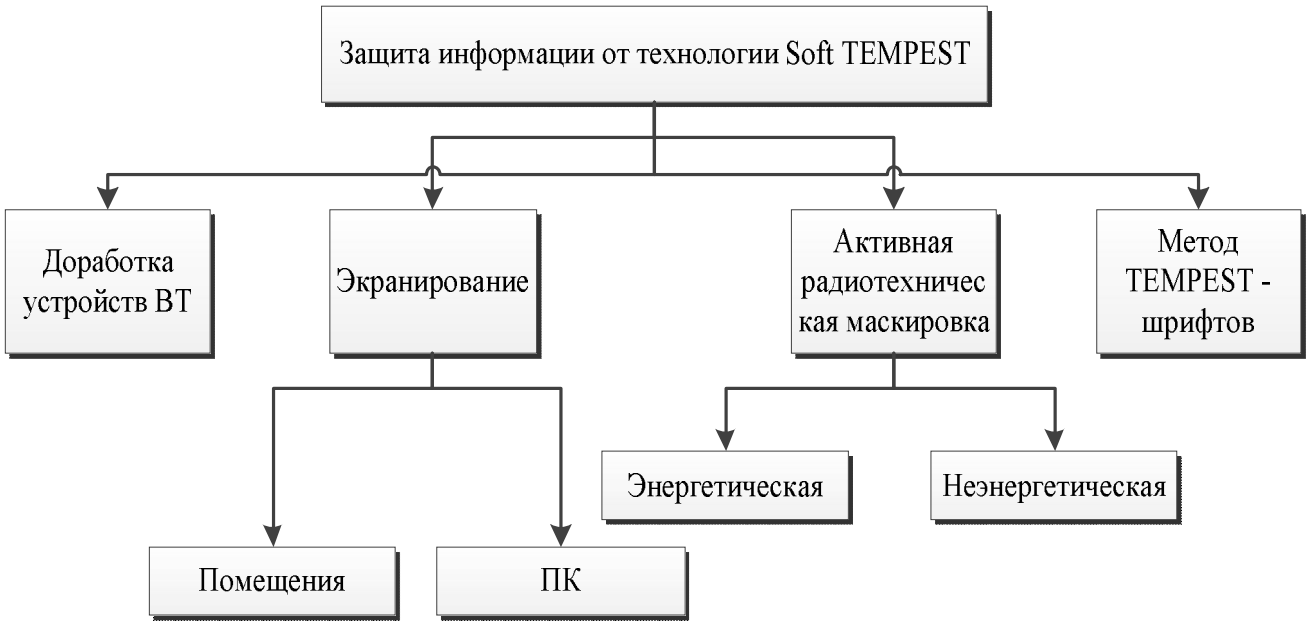

Рис. 2. Защита информации на ПК от технологии SOFT TEMPEST

1) Доработка устройств ВТ(вычислительной техники) с целью минимизации уровня излучений осуществляется специализированными организациями. Используя различные радиопоглощающие материалы и схемотехнические решения, удается существенно снизить уровень излучений ВТ. Стоимость подобной доработки зависит от размера требуемой зоны безопасности и колеблется в пределах 20-70% от стоимости ПК.

2) Электромагнитная экранировка помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат и не всегда возможна по эстетическим и эргономическим соображениям, но достаточна эффективна.

Экранирование компьютера даже с применением современных технологий - сложный процесс, потому что излучения для каждого компьютера сугубо индивидуальное. В излучении одного элемента преобладает электрическая составляющая, а в излучении другого – магнитная, следовательно необходимо применять разные материалы. У одного монитора экран плоский, у другого - цилиндрический, а у третьего с двумя радиусами кривизны. Поэтому реально доработка компьютера осуществляется в несколько этапов. Вначале осуществляется специсследование собранного компьютера. Определяются частоты и уровни излучения. После этого идут этапы анализа конструктивного исполнения компьютера, разработки технических требований, выбора методов защиты, разработки технологических решений и разработки конструкторской документации для данного конкретного изделия (или партии однотипных изделий). После этого изделие поступает собственно в

производство, где и выполняются работы по защите всех элементов компьютера. После этого в обязательном порядке проводятся специспытания, позволяющие подтвердить эффективность принятых решений. Если специспытания прошли успешно, заказчику выдается документ, дающий уверенность, что компьютер защищен от утечки информации по каналам побочного радиоизлучения.

3) Активная радиотехническая маскировка предполагает формирование и излучение в непосредственной близости от ВТ маскирующего сигнала.

При энергетической маскировке излучается широкополосный шумовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучений ПК. Одновременно происходит наводка шумовых колебаний в отходящие цепи. Из устройств активной энергетической маскировки наиболее известны: "Гном", "Шатер", "ИнейТ, "Гамма". Их стоимость достигает 25- 30% от стоимости ПК.

Неэнергетический, или его еще можно назвать - статистический. Исходной предпосылкой в данном методе является случайный характер электромагнитных излучений ПК. Сформированный с помощью оригинального алгоритма сигнал излучается в пространство компактным устройством, которое может устанавливаться как на корпусе самого ПК, так и в непосредственной близости от него. Не создают ощутимых помех для других электронных приборов, находящихся рядом с ними, что также является их неоспоримым преимуществом.[4]

4) Метод TEMPEST-шрифтов заключается в удалении из шрифтов верхних 30% спектра горизонтальной частоты. Так как большинства установок могут принимать информацию, представляемой в спектре Фурье частотами из диапазона $0.7*fp/2 < f <= fp/2$. В отфильтрованный текст потери в качестве текста обычно почти незаметны пользователю на экране компьютера. Ограниченный фокус электронного луча, ограниченное разрешение глаза, а также эффекты, порождаемые маской и электроникой монитора, всячески фильтруют этот сигнал.[2]

Вывод. Универсального, на все случаи жизни, способа защиты информации от перехвата информации через ПЭМИН ПК, в частности монитора использую технологию Soft TEMPEST, конечно же, не существует. В каждом конкретном случае специалистами должно приниматься решение о применении того или иного способа защиты, а возможно и их комбинации. И все же для большинства малых и средних фирм оптимальным способом ЗИ с точки зрения цены, эффективности защиты и простоты реализации представляется активная радиотехническая маскировка.

ЛИТЕРАТУРА:

1. Soft Tempest Hidden Data Transmission Using Electromagnetic Emanations / M.Kuhn,R.Anderson).
2. Ю.А. Шерстнёва, Россия, Москва, МИФИ (технический университет), Защита информации от утечки по техническим каналам(современный зарубежный опыт)
3. В.В. Овсянников, Г.Т. Солдатенко. Нужны ли нам защищенные компьютеры? Научно - методическое издание "Техника специального назначения", 2001, №1.
4. http://www.support17.com/component/content/39.html?task=view
5. Программный Темпест: скрытная передача данных с помощью электромагнитных излучений, Маркус Г. Кун и РоссДж. Андерсон (Компьютерная лаборатория университета Кембридж, Великобритания)

Надійшла: 12.05.2012
Рецензент: д.т.н., проф. Юдін О.К.