СЕКЦИЯ «ПРИКЛАДНОЙ АНАЛИЗ ДАННЫХ»

ИССЛЕДОВАНИЯ ЭЛЕКТРОМАГНИТНОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Xiong Shuai, В.Э. Яскевич

Белорусский государственный университет, г. Минск, Беларусь
E-mail: Yaskevich_VE@bsu.by

Исследования посвящены оценке угрозы утечки информации, обрабатываемой современными вычислительными средствами, по электромагнитному каналу. Проблема известна десятки лет. Однако, раньше так называемые TEMPEST атаки были уделом дорогостоящих средств иностранной технической разведки. Развитие современных приемных устройств, программно-определяемых приемников (SDR), анализаторов спектра реального времени сделало такую атаку гораздо доступнее. Это может существенно изменить модель нарушителя и перечень угроз как для информационных систем, так и для объектов информатизации. В докладе представлены методика исследований электромагнитного канала утечки информации средств вычислительной техники и результаты экспериментальных исследований.

Ключевые слова: электромагнитный канал утечки информации средств вычислительной техники.

ВВЕДЕНИЕ

Формирование электромагнитного канала утечки информации можно считать завершенным при обеспечении условий размещения приемника, его технических характеристик и параметров, а также выборе наиболее подходящей антенной системы. В последнее время появилось ряд публикаций, описывающих формирование электромагнитного канала утечки информации для VGA интерфейса на основе общедоступных устройств, включая программно-определяемые радиоприемники (SDR) [1, 2, 3]. Однако все они представляют попытку прямого представления изображения монитора, не учитывая потенциальные возможности последующей обработки зарегестрированных сигналов. Представленные исследования направлены на оценку степени угрозы утечки информации по электромагнитному каналу при использовании анализаторов спектра реального времени, выполненных в виде USB приставок, позволяющих записывать IQ сигналы электромагнитных излучений мониторов.

МЕТОДИКА ИССЛЕДОВАНИЙ

В качестве источника побочных электромагнитных излучений (ПЭМИ) VGA интерфейса использовался настольный компьютер с ЖК-

монитором. Излучателем электромагнитных волн в этом случае, в основном, являлся VGA кабель.

Магнитная антенна для приема ПЭМИ была изготовлена из медной трубки, одного витка провода и согласующего трансформатора 9:1. Выбор магнитной антенны обусловлен сложной электромагнитной обстановкой в месте проведения исследований: условия города и учебного корпуса с множеством лабораторий.

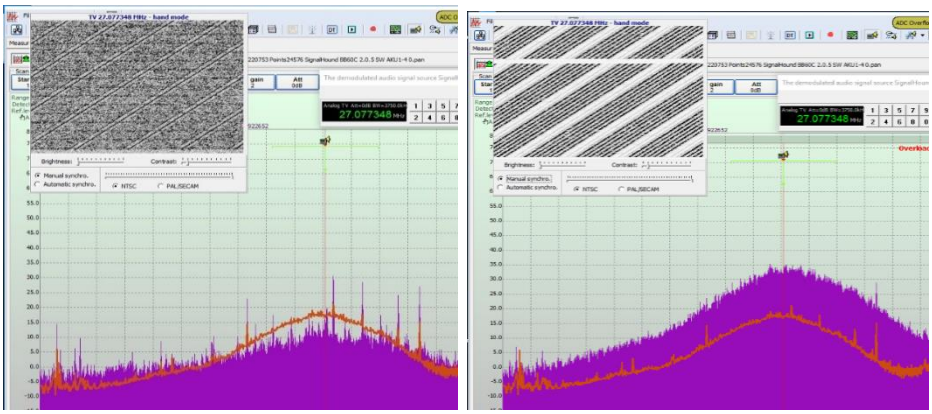
В качестве приемных устройств использовались анализатор спектра реального времени BB60C (The Signal Hound) и RSA306B (Tektronix). Оба анализатора являются USB приставками и требуют высокоскоростного интерфейса и управляющих программ.

Анализатор спектра BB60C работал под управлением программы RadioInspectorRT (ООО «РадиоСофт», г. Москва), реализующей функции радиомониторинга и имеющей в своем составе детектор аналогового телевизионного сигнала. Именно в качестве аналогового телевизионного приемника с возможностью ручной синхронизации он и использовался.

Анализатор спектра RSA306B работал под управлением штатной программы Tektronix SignalVu-PC. Этот анализатор использовался для регистрации IQ сигналов ПЭМИ VGA интерфейса с целью последующей обработки полученных записей.

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ

На рис. 1 представлены результаты регистрации ПЭМИ VGA кабеля с помощью анализатора спектра BB60C и программного обеспечения RadioInspectorRT, работающего в режиме детектора аналоговых телевизионных сигналов. На экране исследуемого монитора специальным программным обеспечением формировалось шесть чередующихся белых и черных вертикальных полос, одинаковой ширины, равномерно заполняющих экран (рис. 1 а) представляет принятый сигнал от черного экрана. Даже при отсутствии изображения работают сигналы синхроимпульсов и приемное устройство удалось синхронизировать с помощью ручного управления. На рис. 1 б) мы видим несколько отображений исследуемого экрана с вертикальными полосами. Отображение нескольких экранов, а также наклон вертикальных полос обусловлен различной частотой строчной и кадровой разверток исследуемого монитора и стандарта NTSC, который реализуется TV детектором приемного устройства. Ниже изображения экрана на рис. 1 представлен спектр радиосигнала при черном экране и вертикальных полосах. Красная линия (так называемый порог обнаружения) занимает на обоих рисунках а) и б) неизменное положение и служит для визуальной оценки увеличения уровня сигнала при отображении полос на экране.



а *б*

Рис. 1. Регистрация изображения монитора детектором телевизионных сигналов:
а - черный экран; *б* - 6 вертикальных полос

На рис. 2 представлен прием ПЭМИ VGA интерфейса при отображении на исследуемом мониторе слова «PEACE» с размером шрифта 300 пикселей. Различие в кадровых и строчных частотах привело к разрыву слова и смещения конца слова в начало.

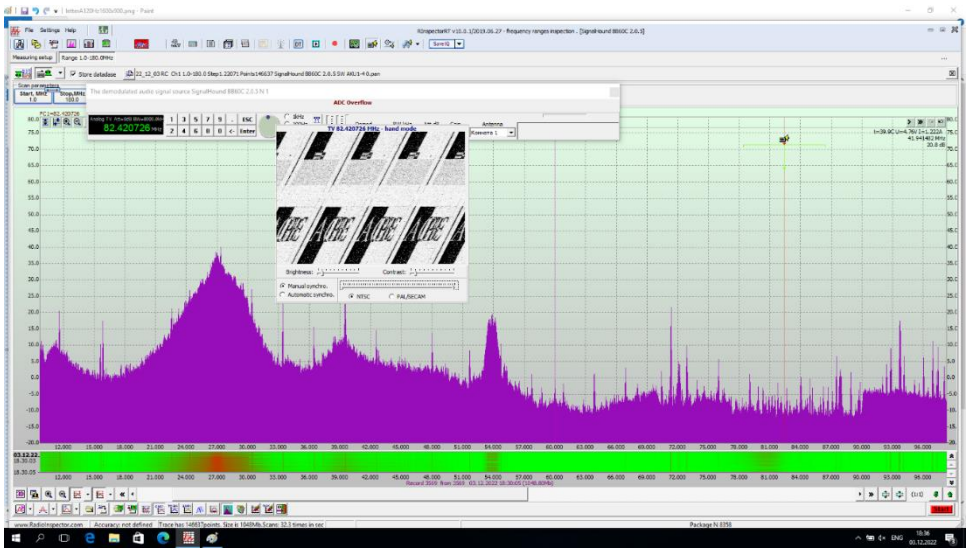


Рис. 2. Регистрация изображения слова PEACE

На рис. 3 представлен фрагмент записи сигналов ПЭМИ при отображении 6 белых вертикальных полос на черном экране. Запись IQ сигналов выполнена с помощью анализатора RSA306B и программного обеспечения SignalVu-PC. На рис. 3 отображены значения корней из суммы квадратов IQ сигналов (мгновенные значения амплитуд). На фрагменте показаны 6 линий развертки монитора. В каждой линии просматриваются сигналы от 6 вертикальных полос. При получении записи VGA сигнала всегда возникает вопрос

синхронизации как по строкам, так и по кадрам. На рисунке 4 показан результат расчета автокорреляционной функции представленного фрагмента. Максимумы автокорреляционной функции позволяют обеспечить требуемую синхронизацию.

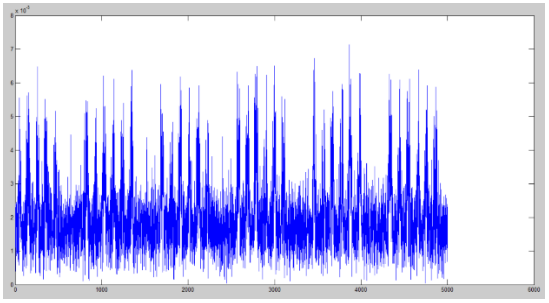


Рис. 3. Фрагмент записи 6 линий

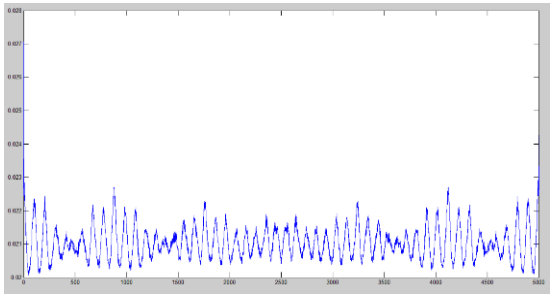


Рис. 4. Автокорреляционная функция

ВЫВОДЫ

Представленные результаты исследований подтверждают доступность формирования электромагнитного канала утечки информации на основе общедоступных радиоприемных устройств. Получена прямая регистрация изображения монитора с помощью телевизионного приемника, реализованного на основе анализатора спектра. Выполнена запись IQ сигналов ПЭМИ VGA интерфейса, открывающая новые потенциальные возможности по восстановлению изображений мониторов на фоне шумов.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Markus G. Kuhn*. Compromising emanations: eavesdropping risks of computer displays // Technical Report UCAM-CL-TR-577 University of Cambridge Computer Laboratory, 2003. С. 167.
2. *Martin Marinov*. Remote video eavesdropping using a software-defined radio platform // A dissertation submitted to the University of Cambridge in partial fulfilment of the requirements for the degree of Master of Philosophy in Advanced Computer Science, 2014. С. 68.
3. *Asanka Sayakkara, Nhien-An Le-Khac, Mark Scanlon*. Accuracy Enhancement of Electromagnetic Side-Channel Attacks on Computer Monitors.