Из них ложных срабатываний	4	2	2	3
Найдено правильно	78	59	23	37
Пропуски	35	37	89	75
Из них по причине отсутствия в базе	32	24	85	29
Из них вызванные необходимостью аутентификации	0	0	2	18
По другим причинам	3	13	2	28

Литература

1. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей // Горячая линия – Телеком. – М.: 2014.– 644с.
2. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия// Сборник научных трудов. Российская Академия Наук (М.), Институт системного анализа; ред. Д. С. Черешкин [и др.]. – М. :Ленанд, 2009. – С. 104 – 146.
3. Макаров А. С., Миронов С. В., Цирлов В. Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2005. № 5. С. 109–122.
4. Применение сканеров для анализа защищенности компьютерных сетей // Материалы курса. М.: Учебный центр «Информзащита», 2006.

COMPARATIVE EVALUATION OF THE SECURITY SCANNERS PERFORMANCE DURING THE CONTROL OF LOCAL AREA NETWORKS PROTECTION.

Student Akulov N.V.

National research University «Moscow Institute of electronic technology»

There is considered the method of evaluating the performance of security scanners during the control of local networks protection in this article. The methodology of comparative evaluating the performance of security scanners during the control of local networks protection is proposed. By the results of this evaluation the applicability of the scanner for completing its tasks is described.

МЕТОД ОТЛОЖЕННОГО АНАЛИЗА СИГНАЛОВ ПЭМИН В ЗАДАЧАХ ОЦЕНКИ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФОРМАЦИИ

к.т.н. Бонч-Бруевич А.М., асп. Анженко А.А.

Московский государственный технический университет им. Н.Э. Баумана

Побочные электромагнитные излучения и наводки от средств вычислительной техники являются одним из возможных каналов утечки информации ограниченного доступа.

Исследованию ПЭМИН на сегодняшний день посвящено множество публикаций как отечественных (Хорев А.А. [3], Суворов П.А., Кондратьев А.В.), так и зарубежных авторов (Вима Ван Эйк [1], М.Г. Кюн [2]).

Целью данной статьи является описание метода отложенного анализа сигналов ПЭМИН и описание его применения в задачах оценки защищенности телекоммуникационной информации.

Существующие методики оценки защищенности информации от утечки по каналу ПЭМИН не учитывают возможности отложенного анализа записанных сигналов. Вместе с тем, современные средства измерений и системы сбора данных (AgilentTechnologies и X-COM Systems) позволяют решать трудоемкую и вычислительно сложную задачу согласованной фильтрации в режиме отложенного анализа. То есть проводить запись сигнала с антенны в полосах частот от 3 Гц до 50 ГГц с полосой пропускания до 160 МГц в течение 6 часов с возможностью последующей обработки и воспроизведения. Программное обеспечение этих средств измерений позволяет проводить поиск по определенным критериям в записанных сигналах, а также отображать сигналы в частотной и временной областях. Кроме этого возможно масштабирование системы и осуществление разнесенного приема или расширения полосы анализа.

Существующие возможности позволяют выбрать оптимальный алгоритм обработки для обнаружения информативных сигналов. Обработка записанных сигналов позволяет решать задачу различения информационных сигналов от различных устройств, за счет того, что основное влияние на частоты локальных максимумов спектра оказывают параметры фронта и спада импульсов. Уменьшение времени фронта и спада импульсов приводит к увеличению уровня ПЭМИ, а даже незначительное изменение этих характеристик сигнала будет приводить к изменению частот локальных максимумов спектра.

Известно, что индивидуальные особенности имеют фронты электрических импульсов, положительные при переходе от "0" к "1" и отрицательные при переходе от " 1" к "0". Поэтому с точки зрения возможностей перехвата информации прием излучений, соответствующих фронтам импульсов, вызывает особый интерес. Длительность и форма фронта зависят от особенностей конкретной микросхемы и параметров соединительных цепей. При излучении происходит фильтрация, приводящая к тому, что форма импульса в эфире резко отличается от "ступенчатой функции".

В основе подходов к оценке эффективности защиты информации от утечки по каналу ПЭМИН должна быть предусмотрена методика оценки потенциальной возможности нарушителя выполнить согласованную фильтрацию пачки из нескольких последовательно идущих импульсов. Учет этой возможности означает необходимость принципиально отличается от действующих методик оценки защищенности, так как согласно методикам оценивается только не превышение сигнала ПЭМИН над уровнем фона. В результате измерений не всегда удается определить, насколько фоновые шумы оказываются выше по уровню чем излучение опасного сигнала, а если превышение незначительное то согласованная фильтрация пачки из нескольких импульсов обеспечивает возможность восстановления сигнала, уровень которого ниже уровня шумов.

Учитывая перспективность данного направления, в МГТУ им. Н.Э. Баумана был разработан измерительный комплекс для отложенного анализа сигналов ПЭМИН.

1. Описание комплекса отложенного анализа

Комплекс предназначен для проведения измерений, записи и отложенного анализа сигналов ПЭМИН.

Данный комплекс позволяет осуществить полный цикл работ по инструментальному исследованию технических средств, включая поиск, запись и обнаружение информационных составляющих ПЭМИН, а так же измерение их параметров.

Комплекс обеспечивает проведение исследований по каналам ПЭМИН в автоматическом режиме и в режиме ручного управления оператором (экспертный режим).Комплекс построен по блочно-модульному типу (рисунок 1). Основные составные части комплекса представляют собой приборы различного назначения. Составные части изделия соединяются между собой с помощью радиочастотных и интерфейсных кабелей. Взаимодействие составных частей комплекса осуществляется под управлением оператора.

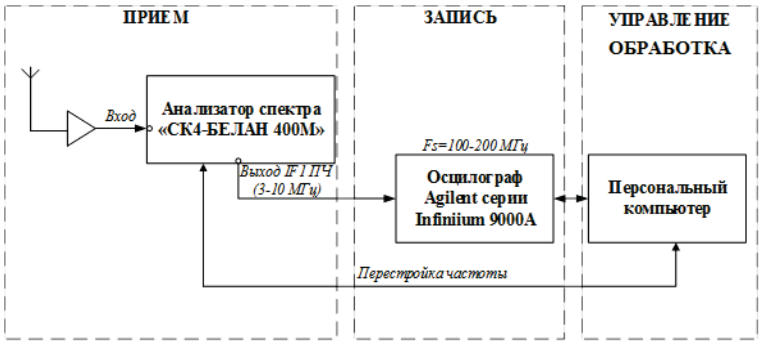

Рис. 1. Структурная схема измерительного комплекса отложенного анализа сигналов ПЭМИН

Комплекс состоит из измерительных антенн (антенна широкополосная измерительная дипольная активная и антенна широкополосная измерительная рамочная активная), измерительного приемника (анализатора спектра), цифрового осциллографа, и персональной электронной вычислительной машины (ПЭВМ). В качестве прикладного программного обеспечения используется пакет программ MATLB-Simulink и пакет программ MicrosoftOffice 2013.

2. Анализ записанных сигналов в программе MATLAB

Процедуре записи предшествует операция поиска, осуществляемая путем перестройки частоты анализатора спектра (рисунок 2)

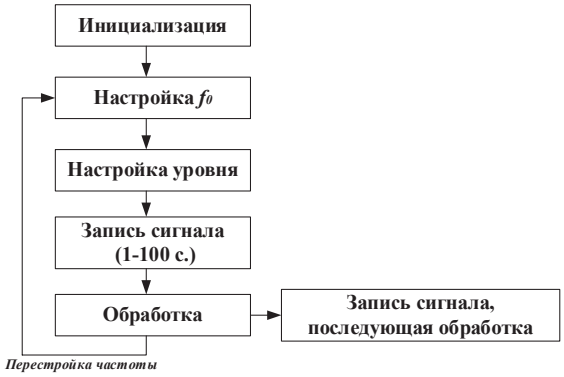

Рис. 2. Блок-схема алгоритма записи сигналов ПЭМИН

Отложенный анализ записанных сигналов ПЭМИН осуществляется программой MATLAB по следующему алгоритму:

1. Импорт данных из текстового файла;
2. Инициализация переменных (массивы данных, параметры фильтра, частота дискретизации, промежуточная частота, разрядность, длина блока данных и др.);
3. Фильтрация и перенос спектра сигнала;
4. Децимация;
5. Построение спектра.

В качестве примера результатов измерений ПЭМИН методом отложенного анализа могут служить спектрограммы, представление на рисунках 3, 4, 5. На рисунке 3 видно отдельные кадры длительностью 0,16 с., выводимые на экран монитора компьютера. На рис. 5 представлена спектрограммы апериодического сигнала ПЭМИН.

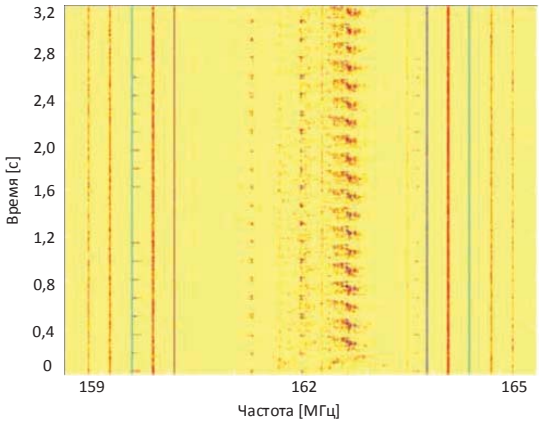

Рис. 3. Спектрограмма сигнала ПЭМИН монитора компьютера

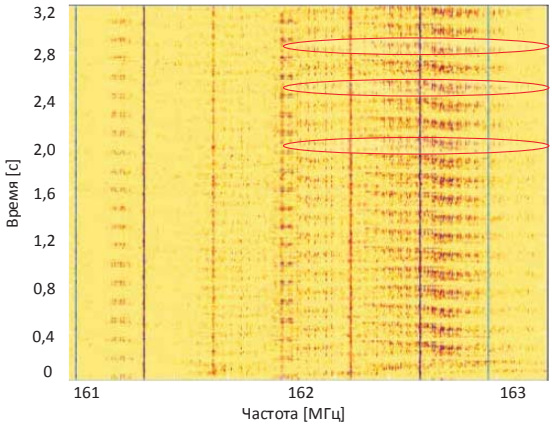

Рис. 4. Спектрограмма сигнала ПЭМИН монитора компьютера

(краснымвыделеныобластикадра)

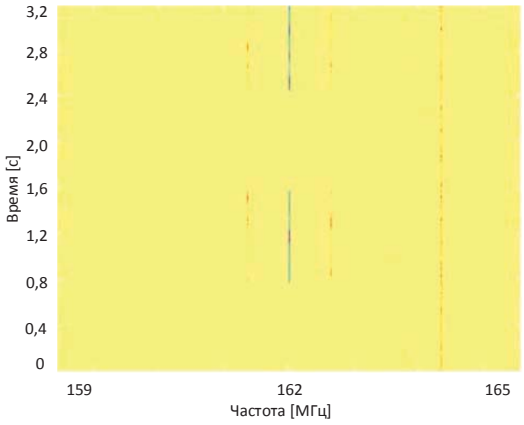

Рис. 5.Апериодический сигнал ПЭМИН

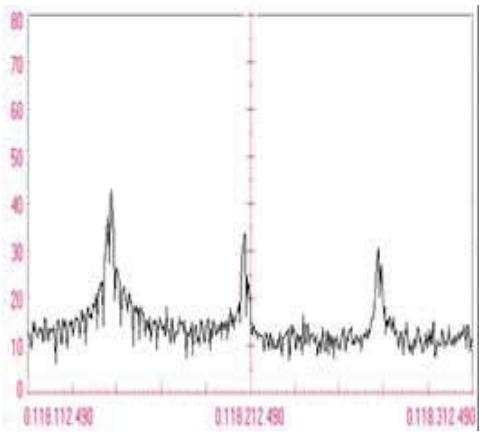

Рис. 6. Сигнал ПЭМИН монитора на экране типового автоматизированного комплекса

В качестве преимущества такого вида анализа перед современными автоматизированными комплексами измерений ПЭМИН (рисунок 6), можно выделить возможность корреляционного анализа изображений спектрограмм сигналов ПЭМИН во временной области. Данный метод так же может быть применим для анализа апериодических и одиночных (импульсных) сигналов ПЭМИН.

Выводы:

- Для оценки защищенности информации от утечки за счет ПЭМИН предложен более перспективный метод отложенного анализа сигналов ПЭМИН.
- Проведено описание метода отложенного анализа и рассмотрена структурная схема стенда для отложенного анализа сигналов ПЭМИН.
- Среди направлений дальнейших исследований можно выделить: исследование ограничений применения комплекса, оценка чувствительности измерительного тракта, а так же оценка погрешностей измерений.
- Ожидается, что в результате дальнейших исследований методом отложенного анализа удастся повысить точность анализа спектра и оценки временных параметров сигнала по сравнению с непосредственными измерениями при помощи анализатора спектра, поскольку анализ записи сигнала позволяет проводить больше циклов усреднения, чем прямые измерения.

Литература

1. Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. http://cryptome.org/emr.pdf.
2. Kuhn G. Compromising emanations: eavesdropping risks of computer displays: This technical re- port is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf.
3. А.А. Хорев. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера// Специальная техника. 2011, No 1. С. 47–49.

METHOD OF DELAY SIGNAL ANALYSIS COMPROMISING EMANATIONS IN PROBLEMS OF INFORMATION SECURITY TELECOMMUNICATIONS

Ph.D.Bonch-Bruevich A.M., postgraduate Anzhenko A.A.

National research University «Moscow Institute of electronic technology»

The problems associated with the analysis of signals by compromising emanations (TEMPEST). Describes the potential of the method of recordingand delay signal analysis. Is a block diagram of the standdelay signal analysis, the algorithm analyzes the recorded signals.

ИССЛЕДОВАНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ВИДЕОСИСТЕМЫ С ИНТЕРФЕЙСОМ LVDS

студ. А.С. Баталов

Национальный исследовательский университет «Московский институт электронной техники»

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами. ПЭМИН способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах.

Из всех трактов современных ПЭВМ наибольшую опасность с точки зрения утечки по этому каналу представляют тракты отображения графической информации. Возможность перехвата вероятным злоумышленником излучаемой этими трактами информации во многом определяет облик системы защиты информации.

Исторически сложилось так, что LVDS (LowVoltageDifferentialSignaling)стал, де-факто, стандартом для подключения ЖК панелей мониторов и ноутбуков, соответственно именно он и применяется в большинстве стандартных ЖК панелей для получения данных [1].

LVDS означает передачу информации дифференциальными сигналами малых напряжений. Это направление передачи данных использует очень малые перепады дифференциального напряжения (до 350 мВ) на двух линиях печатной платы или сбалансированного кабеля.

Для проводимых исследований была выбрана ПЭВМ ТЕЦА.469536.032-02, производимая на предприятии ЗАО «НТЦ ЭЛИНС».

Переносная ЭВМ (рисунок 1) предназначена для организации интерфейса оператора в системах подготовки данных и управления, а также для решения задач сопровождения и управления объектами в реальном режиме времени.

Характеристики ПЭВМ [2]:

- Тип центрального процессора Intel X86 Core 2Duo (1500 МГц);
- Кэш второго уровня 4 Мбайт;
- ОЗУ 2 Гбайт;
- Видеопамять 128 Мбайт;
- Встроенный Flash-диск не менее 160 Гбайт;
- Монитор ЖКИ-TFT;
- Диагональ 15";
- Разрешение 1024 x 768 пикселей;
- Глубина цвета 32 бита;
- Яркость 800 кд/м2;
- Контраст 800:1;

Рис. 1– Внешний вид ПЭВМ ТЕЦА.469536.032-02