объекта в соответствии со структурой плоскости Паскаля. Следует отметить, что формализацию ряда параметров, например защитных свойств местности, целесообразно осуществлять по правилам нечетких множеств. Тогда решение о выборе очередного шага должно формироваться на основе аппарата нечеткой логики.

Моделирование процесса движения сил реагирования, выполняющих задачу пресечения действий нарушителя, следует осуществлять аналогичным образом, с применением сети Петри, структура которой приведена на рис. 4.

В настоящее время разрабатывается программное обеспечение, предназначенное для статистического формирования оценки эффективности СФЗ путем многократного запуска сети.

Библиографические ссылки

1. *Духан Е. И., Давлетханов Р. Р.* Развитие вероятностного подхода к оценке эффективности систем физической защиты // Современные охранные технологии и средства обеспечения комплексной безопасности объектов : тез. докл. IX Всерос. науч.-практ. конф. (Пенза – Заречный, 18–20 сентября 2012 г.) Пенза : Изд-во ПГУ, 2012. 454 с.

2. *Леоненков А. В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб. : БХВ-Петербург, 2005. 736 с.: ил.

ИССЛЕДОВАНИЕ КАНАЛОВ ПЭМИН ПРИ ПОМОЩИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «СИГУРД»

И. Ф. Файсханов, А. С. Лучинин
(Екатеринбург, УрФУ, f_irek@mail.ru)

Информационная безопасность на сегодняшний день является ключевым фактором в жизни общества. Фраза «кто владеет информацией – тот владеет миром» становится актуальной на сегодняшний день. Широкое развитие компьютерных систем облегчает работу, получение информации становится болес доступным, обработка более удобной, хранение информации – централизованным.

Однако порой обработке подвергается информация, которую необходимо сделать доступной лишь для определенного круга лиц. На этом этапе и встает вопрос об обеспечении безопасности информации в системах информатизации.

Один из наиболее уязвимых каналов – канал побочных электромагнитных излучений и наводок (ПЭМИН), образующийся при функционировании радиоэлектронных средств. Наибольшую опасность представляют собой излучения средств, обрабатывающих конфиденциальную информацию. Часто к ним относится вычислительная техника и средства связи [1].

При помощи паразитных связей и наводок сигналы со средств, обрабатывающих конфиденциальную информацию, могут попадать на вспомогательные устройства и системы, такие как системы пожарной и охранной сигнализаций, системы обогрева и др.

На сегодняшний день внимание уделяется побочным электромагнитным излучениям вычислительных средств, в первую очередь персональным компьютерам (ПК). Рассматриваются излучения интерфейсов, клавиатуры, процессора, жесткого диска, принтера и видеосистемы.

Наиболее уязвимы в данном вопросе видеосистема и клавиатура. Это обусловлено следующими факторами:

1. Структура сигналов клавиатуры и видеосистемы известна;

2. Длительное время работы данных устройств позволяет злоумышленнику настроить аппаратуру перехвата.

В ходе работы было проведено исследование побочных электромагнитных излучений (ПЭМИ) видеосистемы персонального компьютера. Для обнаружения, измерения и оценки сигналов в данной работе применялся программно-аппаратный комплекс «Сигурд». Данный комплекс включает (рис. 1, 2):

1. Персональный компьютер;

2. Анализатор спектра;

3. Комплект антенн.

Принцип работы следующий:

1. Оператор запускает приложение «Сигурд-тест» на исследуемом ПК для генерирования тестового сигнала. Приложение вычисляет значение частоты сигнала.

2. На ПК комплекса «Сигурд» запускается приложение «Сигурд-лайт» и находится тестовый сигнал, который, как правило, имеет небольшое отклонение от расчетного.

3. Формируется эталон верификации для поиска сигнала на высших гармониках (рис. 3).

4. Выполняется поиск сигналов с применением антенн для обнаружения электрической и магнитной составляющих.

5. Выполняется верификация сигналов, после которой приложение оставляет сигналы, являющиеся опасными (рис. 4).

6. Выполняется ручная верификация, во время которой оператор контролирует правильность обнаружения сигналов и, при необходимости, вносит корректировки.

7. Выполняется измерение сигналов и шумов.

8. Выполняется расчет зон $R2$, $r1$, $r1'$ с формированием протокола специальных исследований.

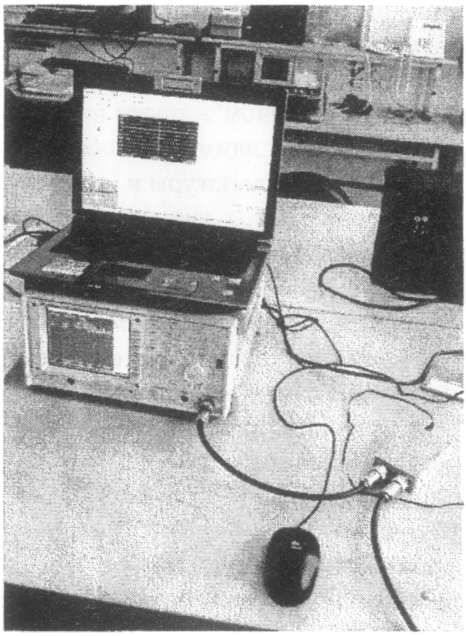

Рис. 1. Персональный компьютер и анализатор спектра

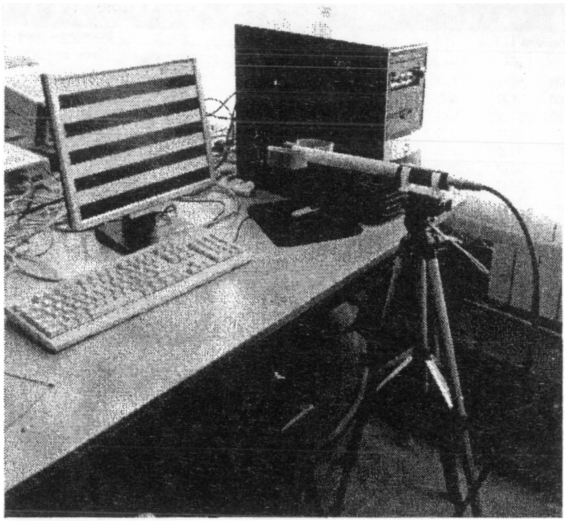

Рис. 2. Антенна для обнаружения электрической составляющей и исследуемый персональный компьютер

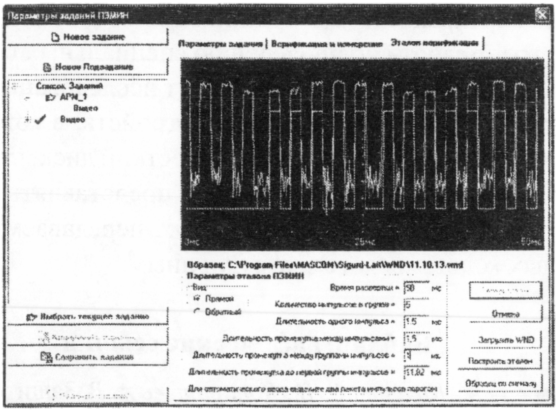

Рис. 3. Формирование эталона верификации

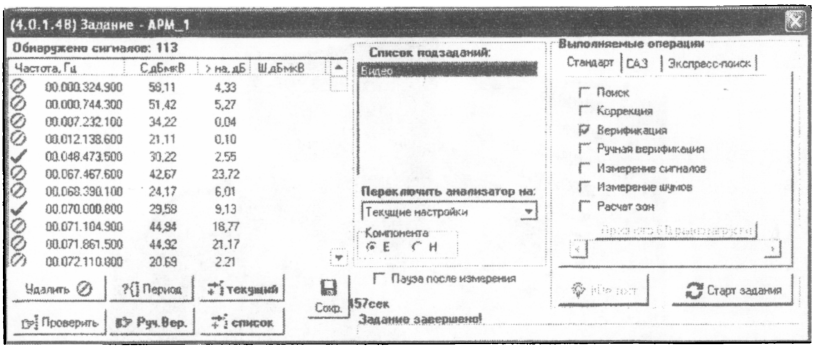

Рис. 4. Верификация. Опасные сигналы отмечены галочкой

В целом данный программно-аппаратный комплекс позволяет с минимальным участием оператора провести специальные исследования достаточно быстро и качественно. Однако стоит отметить и недостатки данного комплекса. Было обнаружено, что при поиске пропускаются некоторые спектральные составляющие, но их удается найти в ручном режиме. Тем не менее достоинства данного комплекса перекрывают недостатки. Таким образом, данный комплекс облегчает работу по проведению специальных исследований.

Дальнейшими целями работы будут исследования ПЭМИ клавиатуры, интерфейса USB, а также устройств, в которых данные передаются параллельными кодами (жесткий диск, принтеры, процессор). Данные исследования будут представлять интерес, поскольку считается, что перехват данных, передаваемых в виде параллельных кодов, является затрудненным.

Библиографические ссылки

1. *Бузов Г. А.*, *Калинин С. В.*, *Кондратьев А. В.* Защита от утечки информации по техническим каналам : учеб. пособие. М. : Горячая линия-Телеком, 2005. 416 с.

2. Программная оболочка «Сигурд-Лайт» : руководство пользователя. [Б. м.] : МАСКОМ, 2006. 46 с.