Література: 1. Герасименко В. А. Защита информации в АСОД (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с. 2. Девянин П. Н., Михальский О. О. и др. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192 с. 3. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия. – Телеком, 2000. – 452 с. 4. Богданов А. М., Корнейко А. В. и др. Моделирование безопасной обработки информации в компьютерных системах. – К.: Наукова думка, 2000. – 160 с. 5. Denning D. E. A lattice model of secure information flow // Coinroun. ACM. – 1976. – V. 19, № 5. – P. 236 – 243.

УДК.681.324

МЕТОДИКА АВТОМАТИЗИРОВАННОГО ВЫЯВЛЕНИЯ ПОБОЧНЫХ ИНФОРМАТИВНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ СВЯЗИ И ОБРАБОТКИ ИНФОРМАЦИИ

Алексей Богатырев, Владимир Настрадин, Александр Черноног*
*Национальная академия СБ Украины, *ВИТИ НТУУ "КПИ"*

Аннотация: **Рассмотрена методика обнаружения побочного излучения радиотехнических средств, основанная на использовании различия законов затухания электромагнитного поля в ближней, промежуточной и дальней зоне от источника радиоволн.**
Summary: **The technique of detection of accessory radiation of radio engineering resources based on usage of distinction of the laws of fading of an electromagnetic field in short-range, intermediate and far-field region from a source of radio waves is considered.**
Ключевые слова: **Побочные излучения, защита информации, канал утечки информации, метод двух антенн.**

I Введение

Одним из основных каналов утечки информации является канал ПЭМИ (побочных электромагнитных излучений) аппаратуры связи, хранения и обработки информации. Излучения такого рода обусловлены разными факторами, например:

- наличием в схемах генераторов синусоидальных и импульсных сигналов;
- применением нелинейных преобразований высокочастотных сигналов, приводящих к появлению кратных гармоник;
- возникновением при определенных условиях паразитной генерации;
- старением и выходом из строя деталей узлов блокировки, фильтрации по питанию и т. п.;
- недостаточной экранировкой высокочастотных узлов и аппаратуры в целом, окислением в местах механического соединения частей экранировки и т. д.

Как правило, работа любой аппаратуры сопровождается целой гаммой излучаемых частот в очень широком спектре с самой разной интенсивностью, среди которых имеются частоты, модулированные информационной составляющей. Последние представляют реальную опасность, если они имеют за границей контролируемой зоны достаточный для перехвата уровень. В литературе достаточно подробно освещены методики снятия информации с канала побочного излучения, которые используются специалистами как спецслужб, так и промышленного шпионажа. Чем меньше размеры контролируемой зоны, тем жестче требования по соблюдению безопасных норм уровней побочного излучения. Поэтому задача своевременного обнаружения побочного излучения аппаратуры связи, хранения и обработки информации всегда представлялась весьма актуальной и является одной из основных составляющих комплекса мероприятий по защите информации.

II Постановка задачи

Задача обнаружения побочного излучения радиотехнических средств во всех случаях представляет собой многоальтернативную задачу обнаружения сигнала с заранее неизвестными параметрами: частотой, амплитудой, шириной спектра и т. д.

На практике применяются разные методики, использование которых в основном требует специального дорогостоящего оборудования и больших затрат времени. Например, один из традиционных путей решения задачи обнаружения побочного электромагнитного излучения включает в себя:

– теоретическое определение возможных источников излучения;
– составление каталога возможных частот излучения от данного радиотехнического комплекса, в котором указываются возможный уровень излучения, вид модуляции и ширина спектра сигнала;
– сопоставление теоретических данных с данными, полученными практически в специальной экранированной комнате (при наличии таковой).

На основе этих данных регулярно по плану регламентных работ производится нацеленный поиск побочных электромагнитных излучений.

Недостатком такого метода является возможность необнаружения новых излучений на частотах, отличных от указанных в каталоге, хотя побочные излучения могут возникнуть из-за возбуждения апериодических усилительных каскадов, согласующих и других элементов и узлов. Частоты подобных излучений определяются как монтажными и паразитными емкостями и индуктивностями, так и типом применяемых активных элементов и могут возникать в самых неожиданных местах. Излучения паразитного характера регистрировались неоднократно, например, в аппаратуре каналовыделения на частоте 130 МГц. Источником генерации являлся УНЧ.

Паразитные излучения такого рода представляют повышенную опасность в том плане, что они, как правило, модулируются принимаемым сигналом.

Сложность обнаружения таких излучений в том, что они зачастую не оказывают существенного влияния на работу каскадов (узлов), в которых возникают. Изделие в целом остается работоспособным и продолжает выполнять свои функции. Поэтому, естественно, встает задача непрерывного отслеживания информативных побочных излучений технических средств.

Основная проблема традиционных методик состоит в трудности идентификации сигналов побочного излучения на фоне реальных сигналов в эфире.

Наиболее современные технологии поиска ПЭМИ на настоящий момент реализованы:

- в комплексах RS-1100, RS-1200 (которые с успехом используются и для поиска радиозакладок);
- в комплексе АСТРА;
- в комплексе АКОР-1.

Как известно, наибольшую вероятность обнаружения сигнала дает система, настроенная на конкретный сигнал с заранее известными признаками. В этом случае задача многоальтернативного обнаружения сводится к простой задаче бинарного типа: «сигнал есть/сигнала нет». Для реализации подобной задачи необходимо "ввести" в побочное излучение определенный признак, а затем, выявляя на выходе приемного тракта наличие этого признака, с вероятностью, близкой к 1, установить факт существования побочного излучения.

При своей эффективности упомянутые комплексы требуют для идентификации ПЭМИ исследуемой аппаратуры вводить в нее различные тестовые сигналы, а это требует на время проверки снимать аппаратуру с выполнения задания, т. е. временно прекращать ее прямую деятельность. Во-первых, это предполагает некую непостоянность, периодичность (регламентность) ее проверки, а, во-вторых, нет гарантии, что примененные тестовые сигналы выявят на 100% все ПЭМИ данной аппаратуры. Это все усложняется при работе на узлах связи и обработки информации, имеющих в своем составе достаточно много разной техники.

Нами была поставлена задача разработать методику, позволяющую проводить постоянное наблюдение на узлах и автоматизировать обнаружение ПЭМИ без выключения исследуемой аппаратуры практически в момент их возникновения.

III Основная часть

В результате проведенных исследований был разработан принцип обнаружения побочных излучений методом двух антенн, сущность которого заключается в использовании законов затухания электромагнитного поля в зависимости от расстояния от источника излучения. Метод двух антенн сам по себе не нов, но предложенный подход к обработке его результатов позволяет решить поставленную задачу. Известно, что в зависимости от соотношения r/λ, (где r – расстояние от источника излучения до точки измерения, λ – длина волны излучения), электромагнитное поле в точке приема может носить характер либо поля в ближней зоне (при $r \leq \lambda/2\pi$), либо поля в промежуточной зоне (при $\lambda/2\pi \leq r \leq \lambda$), либо поля в дальней зоне (при $r > \lambda$).

Напряженность электромагнитного поля E для этих зон определяется по формуле:

$$E = \frac{A}{r^n},$$

где в ближней зоне n=3, в промежуточной зоне n=2, в дальней зоне n=1, A – величина постоянная для данной частоты и размеров излучателя.

Если на расстояниях r_1 и r_2 от источника излучения установить идентичные антенны $A1$ и $A2$ с действующей высотой $h_д$, то уровни сигналов на выходе антенн соответственно будут равны:

$$U_{\text{вых}A1} = h_д E_1;$$

$$U_{\text{вых}A2} = h_д E_2.$$

Подавая сигнал с этих антенн через антенный коммутатор попеременно (с частотой коммутации F_k) на вход радиоприемного устройства с коэффициентом усиления $K_{ус}$, на его выходе будем иметь:

$$U_{\text{вых}1} = h_д E_1 K_{ус};$$

$$U_{\text{вых}2} = h_д E_2 K_{ус}.$$

Отношение этих напряжений

$$\delta_1 = \frac{U_{\text{вых}1}}{U_{\text{вых}2}} = \frac{h_д E_1 K_{ус}}{h_д E_2 K_{ус}} = \frac{E_1}{E_2} = \frac{r_2^n}{r_1^n};$$

Подставляя $r_2 = r_1 + \Delta r$, будем иметь:

$$\delta = \frac{(r_1 + \Delta r)^n}{r_1^n} \approx 1 + n\frac{\Delta r}{r_1},$$

Δr – разность расстояний между антеннами $A1$ и $A2$.

Таким образом, для всех зон $\delta > 1$, т. е. сигнал от местного источника излучения после антенного коммутатора на входе радиоприемного устройства будет иметь амплитудную модуляцию меандром с частотой коммутации антенн F_k . Глубина модуляции определяется значением δ и, в общем случае, будет иметь максимальные значения в случае расположения антенны $A1$ в ближней зоне источника излучения. В случае же приема сигнала от удаленного источника ($r_1 >> \Delta r$, $\delta \to 1$) глубина модуляции входного сигнала радиоприемного устройства будет иметь весьма малое значение.

Расположение антенн $A1$ и $A2$ относительно исследуемой аппаратуры выбирается из необходимости получения максимального значения Δr. Так Δr будет минимально, когда источник ПЭМИ будет находиться на равном расстоянии от антенн перпендикулярно линии расположения антенн, и Δr будет максимально, когда источник ПЭМИ будет находиться на линии расположения антенн (но не между ними) вблизи А1.

На выходе радиоприемного устройства (после амплитудного детектирования) с помощью компаратора можно выбрать нижний порог срабатывания схемы обнаружения напряжения сигнала с частотой F_k. Тогда можно идентифицировать любое ПЭМИ, возникшее в любой из зон, по наличию в его спектре сигнала с частотой коммутации приемных антенн F_k, а по значению глубины модуляции можно оценивать расстояние r_1 от антенны $A1$ до источника излучения. Регулируя порог срабатывания компаратора можно ограничивать зону обнаружения источника ПЭМИ до размеров контролируемой зоны (чаще всего это ближняя и промежуточная зоны).

Был изготовлен и испытан опытный образец устройства поиска и замера побочных электромагнитных излучений в коротковолновом диапазоне. Функционально оно состоит из следующих узлов: двух идентичных антенн $A1$ и $A2$, антенного коммутатора АК, генератора, радиоприемного устройства РПУ, фильтра частоты F_k с компаратором и ПЭВМ.

Используются активные антенны, представляющие собой медный штырь длиной 0,6 м**,** соединенный с широкополосным антенным усилителем. Входное сопротивление усилителя в рабочем диапазоне частот имеет в основном емкостный характер и образует с емкостным сопротивлением штыря частотно-независимый делитель напряжения.

Максимальное удаление ближайшей антенны ($A1$) от источника ПЭМИ выбиралось из условия обеспечения промежуточной зоны (n=2) для частот верхнего участка КВ диапазона, а дальнюю антенну ($A2$) – на внешней границе контролируемой зоны.

Основные характеристики антенн: диапазон частот 0,1 – 30 МГц, коэффициент усиления по напряжению 12.

Диодный антенный коммутатор имел следующие характеристики: диапазон частот 0,1 – 50 МГц, ослабление по закрытому каналу не менее 60 дБ, ослабление по открытому каналу не более 2 дБ.

Генератор предназначен для управления антенным коммутатором. В его состав входят мультивибратор на частоту 600 Гц и триггер, а также схема, контролирующая работу генератора и вырабатывающая сигнал "авария" в случае его отказа.

Фильтр F_k с компаратором предназначен для выявления сигнала с частотой коммутации антенн и подачи команды на остановку перестройки радиоприемного устройства. При обнаружении сигнала с частотой коммутации обеспечивается звуковая и световая сигнализация. В состав блока обнаружителя входят фильтр, пороговое устройство и схема сигнализации. Выделенный сигнал коммутации выпрямляется, и, если его уровень превышает установленный порог, производятся при необходимости включение сигнализации и выработка напряжения "остановка" для прекращения перестройки приемника. Обнаруженное ПЭМИ замеряется и анализируется. В режиме "измерение" на вход приемника подается напряжение от дальней антенны ($A2$), находящейся вблизи границы охраняемой зоны. Зная коэффициенты передачи антенны, радиоприемника, коммутатора и предварительно откалибровав радиоприемное устройство на данной частоте, определяем напряженность поля побочного излучения

$$E = \frac{U_{\text{вых1}}}{K_{\text{пр}} K_{\text{А}} K_{\text{ком}} h_{\text{д}}}, \left[\frac{\text{мкВ}}{\text{м}}\right],$$

где $K_{\text{пр}}$ – коэффициент передачи радиоприемного устройства; $K_{\text{А}}$ – коэффициент передачи активной антенны; $K_{\text{ком}}$ – коэффициент передачи коммутатора; $h_{\text{д}}$ – действующая высота антенны.

Полученное значение напряженности электрического поля сравнивается с допустимым. Если уровень превышает допустимый, то производится информационный анализ излучения, в результате чего определяется тип аппарата, а затем и сам конкретный аппарат.

В случае автоматического постоянного поиска при обнаружении ПЭМИ ПЭВМ записывает частоту РПУ в таблицу, определяет степень опасности излучения по приведенному выше принципу, записывает полученные данные в таблицу, выделяя степень опасности цветом.

IV Выводы

Проведенные эксперименты подтвердили ожидаемые результаты:

- максимальная чувствительность системы определяется чувствительностью радиоприемного устройства и уровнем сигнала на выходе антенны $A1$;
- при малых значениях ПЭМИ, когда уровень сигнала на выходе антенны $A2$ $U_{\text{вых}A2}$ меньше чувствительности радиоприемного устройства, а на выходе антенны $A1$ $U_{\text{вых}A1}$ выше (что характерно для ближней зоны распространения радиоволн), глубина модуляции сигнала с F_k достигает 100%, что можно использовать как признак того, что уровень излучения ПЭМИ за пределами контролируемой зоны ниже чувствительности радиоприемного устройства, т. е. ниже опасного уровня.
- порог компарации зависит от области исследуемого диапазона радиочастот – на верхних частотах диапазона порог компарации следует снижать. Это объясняется зависимостью размеров ближней, промежуточной и дальней зоны распространения радиоволн от длины волны.

Литература: 1. Я. Л. Альперт, В. Л. Гинзбург, Е. Л. Фейнберг. Распространение радиоволн М., Гос. изд-во технико-теоретической литературы, 1953. 2. М. П. Долуханов. Распространение радиоволн М., "Сов. радио", 1972 – 118 с.

УДК.681.3

БАЗОВА МОДЕЛЬ ЕКСПЕРТНОЇ СИСТЕМИ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Вячеслав Шорошев
НДІ НАВСУ

Анотація: **Розглядається базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах згідно з вимогами національних стандартів ТЗІ України. Обраний Україною шлях наслідування кращого міжнародного досвіду та запобігання їх недолікам щодо комп'ютерної безпеки заслуговує уваги. Прикладом цієї реалізації є нормативні документи НД ТЗІ з**