ТУПОТА Виктор Иванович,
доктор технических наук, старший научный сотрудник
КОЗЬМИН Владимир Алексеевич,
кандидат технических наук, доцент
ТОКАРЕВ Антон Борисович,
кандидат технических наук, доцент

ПРИМЕНЕНИЕ МНОГОФУНКЦИОНАЛЬНОГО КОМПЛЕКСА АРК-Д1ТИ ДЛЯ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПЭМИН

Работа радио- и электротехнических устройств неразрывно связана с появлением в окружающей среде электромагнитных полей (ЭМП). Для некоторых устройств, таких, как радиопередатчики, средства мобильной связи, и т.п., излучение электромагнитных волн является основной задачей; для прочих: компьютеры, сканеры, принтеры и т.д. – возникновение ЭМП является побочным и нежелательным результатом их работы. Подобные паразитные электромагнитные поля, создаваемые устройствами в окружающем пространстве, называют побочными электромагнитными излучениями (ПЭМИ). Кроме того, технические устройства создают электрические наводки на окружающих их проводящих предметах. Существование побочных электромагнитных излучений и наводок (ПЭМИН) делает потенциально возможным перехват информации, обрабатываемой устройством, за счет регистрации и последующей демодуляции этих излучений.

Исследованию ПЭМИН как технического канала утечки информации посвящен ряд публикаций [1, 2]. Вместе с тем параметры устройств, используемых для обработки информации, технические характеристики средств перехвата постоянно совершенствуются, соответственно совершенствуются и нормативно-методические документы (НМД), регламентирующие проверки на ПЭМИН, а потому сохраняется потребность в совершенствовании методов и аппаратуры контроля защищенности информации.

Целью данной статьи является анализ усовершенствований, внесенных в работу сертифицированного программно-аппаратного комплекса АРК-Д1ТИ, для обеспечения его соответствия обновившимся в 2005 г. требованиям НМД в области контроля защищенности информации, обрабатываемой средствами вычислительной техники (СВТ).

Виды специальных исследований и проверяемые каналы утечки информации

При исследовании возможности утечки информации по каналу ПЭМИН обязательными объектами проверки выступают СВТ: рабочие станции, серверы, информационные кабели локальных вычислительных сетей и других технических средств, задействованных для обработки конфиденциальной информации. За счет наводок каналами утечки могут служить также кабели сети электропитания и заземления объекта вычислительной техники, цепи проводных линий связи, пожарной и охранной сигнализации, другие токопроводящие линии и конструкции, например системы отопления, водоснабжения и т. п., имеющие выход за пределы контролируемой зоны объекта информатизации. Выделяют три вида специальных исследований:

- ✗ лабораторные (стендовые) специальные исследования СВТ, направленные на оценку радиуса контролируемой зоны этого СВТ;
- ✗ испытания при контроле защищенности информации на объектах информатизации;
- ✗ исследования, проводимые для оценки эффективности принятых мер защиты информации.

В ходе испытаний подлежат контролю следующие каналы утечки защищаемой информации:

а) побочные информативные электромагнитные излучения СВТ в диапазоне частот 3 кГц…1,8 ГГц, измеряемые с применением электрических антенн, и в диапазоне частот 3 кГц…30 МГц, где измерения проводятся с помощью магнитных антенн;

б) наводки информативных сигналов в диапазоне частот 3 кГц…300 МГц на цепи электропитания и заземления СВТ, а также на отходящие от СВТ цепи, которые выходят за пределы контролируемой зоны объекта вычислительной техники. Измерения наведенных напряжений производятся с помощью специальных активных и пассивных пробников;

в) наводки информативных сигналов в диапазоне частот 3 кГц…300 МГц на сосредоточенные и распределенные случайные антенны, расположенные на объекте. Распределенные случайные антенны (РСА) – это находящиеся вблизи СВТ провода, кабели, проводящие предметы. Сосредоточенные случайные антенны (ССА) – это вспомогательные технические средства. И те, и другие гальванически не связаны с СВТ объекта, но имеют выход за пределы контролируемой зоны.

Основные этапы исследований и показатель защищенности информации

В каждом из упомянутых выше случаев исследование защищенности информации, обрабатываемой СВТ, производится в два этапа. Целью первого этапа является определение частот информативных составляющих ПЭМИ СВТ. Назначение второго этапа – измерение интенсивности найденных составляющих и расчет итоговых показателей защищенности.

Для поиска информативных составляющих ПЭМИ отдельные блоки (узлы) СВТ последовательно друг за другом переводят в специально организуемый тестовый режим работы. В тестовом режиме длительность и амплитуда информационных сигналов блока ВТ остаются теми же, что и в рабочем режиме, но сами сигналы приобретают вид последовательности пачек импульсов, что обеспечивает концентрацию мощности сигналов в узких полосах частот и облегчает выявление спектральных составляющих ПЭМИ.

Показателем защищенности информации служит отношение Δ среднеквадратических значений информативного сигнала E_c и шума $E_ш$. Оно не должно превышать определенного в НМД максимально допустимого отношения информативного сигнал и помехи δ, при котором еще невозможно раскрыть защищаемую информацию

$$\Delta = \frac{E_c}{E_ш} < \delta. \qquad (1)$$

В случаях когда реально наблюдаемое отношение Δ превышает допустимое δ, для обеспечения защищенности информации может быть использована система активного зашумления (САЗ).

Расчет показателя информационной защищенности

Так как побочные электромагнитные излучения аппаратуры, обрабатывающей информацию, практически всегда имеют сложную структуру, то их исследование во временной области оказывается весьма проблематичным. Удобнее производить поиск и анализ составляющих ПЭМИН в спектральной области. Используемые в тестовых режимах сигналы являются периодическими, поэтому их мощность концентрируется в совокупности узкополосных спектральных составляющих, отстоящих друг от друга по оси частот на тактовую частоту тестового сигнала

$$F_T = 1/T \ (Гц), \qquad (2)$$

где T – период следования тактовых импульсов, измеряемый в секундах.

Рассмотрим показанный на *рис. 1* периодический сигнал с длительностью тактовых импульсов равной τ секунд и скважностью $Q = T / \tau$. Средняя мощность этого сигнала может быть вычислена во временной или частотной области. Средняя мощность сигнала во временной области

$$P_{ср} = Э_c/T = Э_c \times F_T = P_и \times \tau \times F_T = P_и/Q, \qquad (3)$$

где $Э_c$ – энергия каждого импульса; $P_{ср}$ – средняя мощность последовательности тактовых импульсов; $P_и$ – средняя мощность сигнала в пределах импульса.

Средняя мощность сигнала в частотной области

$$P_{ср} = 0{,}5 \times \sum_j E_j^2 \qquad (4)$$

где E_j – амплитуда спектральной составляющей сигнала на частоте f_j.

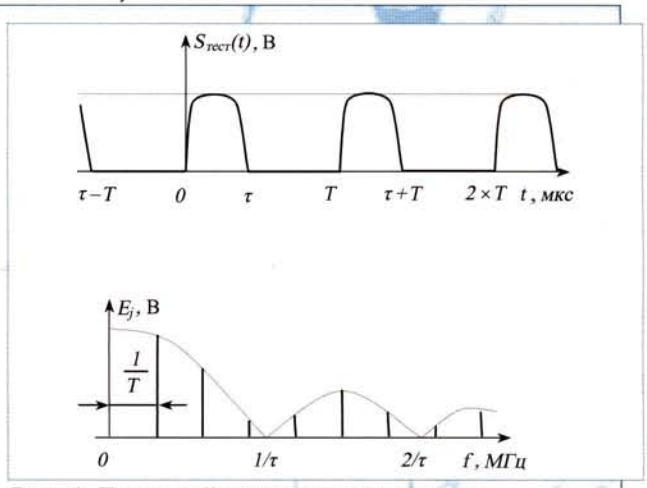

Рис. 1. Тестовый сигнал и его спектр

Приравнивая правые части выражений (3) и (4), для мощности сигнала в пределах импульса получаем

$$P_и = \frac{1}{2F_T\tau} \times \sum_j E_j^2 = \frac{Q}{2} \times \sum_j E_j^2 .$$

В результате среднеквадратическое значение напряженности электромагнитного поля одиночно излученного импульса можно записать в виде

$$E_{ср} = \sqrt{\frac{1}{2F_T\tau} \times \sum_j E_j^2} . \qquad (5)$$

Среднеквадратическое значение напряженности электромагнитного поля нормированных шумов $E_ш$ в полосе $\Delta F = 1/\tau$ составляет при этом

$$E_ш = \sqrt{\int_{\Delta F} E_{шн}^2(f)\,df} , \qquad (6)$$

где $E_{шн}(f)$ – спектральная плотность мощности нормированного значения шума, значение которого определяется НМД.

Итак, отношение среднеквадратических значений информативного сигнала и помехи со спектральных позиций определяется выражением

$$\Delta = \frac{E_{ср}}{E_ш} = \sqrt{\frac{1}{2F_T\tau} \times \sum_j E_j^2} \Bigg/ \sqrt{\int_{\Delta F} E_{шн}^2(f)\,df} . \qquad (7)$$

Это соотношение является базовым для расчета всех показателей информационной защищенности; его уточнение применительно к различным типам специальных исследований будет выполнено ниже.

Использование измерительного комплекса АРК-Д1ТИ при решении задач контроля защищенности информации

Одним из эффективных средств решения задач оценки информационной защищенности является многофункциональный портативный комплекс радиомониторинга АРК-Д1ТИ, сертифицированный Госстандартом России как измерительное средство [4, 6]. Комплекс представляет собой полностью российскую разработку. Он имеет широкие измерительные и функциональные возможности и предназначен для решения задач радио- и радиотехнического контроля. Комплекс в реальном масштабе времени позволяет проводить спектральный анализ радиосигналов с разрешением, изменяющимся от нескольких десятков кГц до десятков Гц, и способен обнаруживать и анализировать сигналы в рабочем диапазоне частот от сотен Гц до 2 ГГц. При использовании конвертера радиосигналов АРК-КНВ4, также являющегося сертифицированным измерительным средством [7], рабочий диапазон комплекса расширяется до 18 ГГц. Высокая чувствительность приемного тракта – около 1 мкВ/кГц^{0,5}, большой динамический диапазон измеряемых уровней сигналов в широкополосном тракте – не менее 70 дБ по интермодуляции 2 и 3 порядка в полосе пропускания 2 МГц – позволяет эффективно решать все задачи контроля защищенности информации, обрабатываемой СВТ.

Программная часть комплекса АРК-Д1ТИ применительно к задачам контроля защищенности информации представляет собой пакет специального математического обеспечения (СМО), который состоит из следующих взаимодействующих программ:

- СМО-ТЕСТЕР – для организации тестовых режимов работы проверяемой аппаратуры (работает в автоматизированном режиме совместно с программой СМО-ДХ);
- СМО-ДХ – для проведения анализа электромагнитной обстановки, включая проводные сети, и выявления побочных электромагнитных излучений СВТ;
- СМО-ПРИЗ – для расчета показателей информационной защищенности.

В 2005 г. в связи с появлением новых НМД программное обеспечение комплекса обновилось: в него вошла модифицированная версия программы проведения анализа электромагнитной обстановки СМО-ДХ и специализированная программа расчета информационной защищенности СМО-ПРИЗ. Программа предназначена для оценки защищенности технических средств и систем обработки информации по требованиям действующих НМД и имеет сертификат [8]. Она позволяет выполнять следующие расчеты:

- радиуса контролируемой зоны средств вычислительной техники, необходимой для предотвращения утечки информации по каналу ПЭМИ;
- показателей защищенности информации, обрабатываемой СВТ, от утечки по каналам ПЭМИН на вспомогательные технические средства и системы;
- оценки эффективности принятых мер защиты информации от утечки по каналу ПЭМИН.

Программа сохраняет результаты измерений и расчетов в собственной базе данных и позволяет формировать соответствующие требованиям НМД протоколы с результатами исследований, сохраняемые в HTML- и RTF-форматах.

Работа комплекса АРК-Д1ТИ при проведении специальных лабораторных исследований СВТ

Рассмотрим особенности совместной работы входящих в пакет СМО программ при проведении специальных лабораторных исследований СВТ. Целью подобных исследований является установление:

- величины максимально возможной зоны перехвата побочных электромагнитных излучений (зоны 2);
- предельных расстояний до вспомогательных технических средств (систем) и их кабельных коммуникаций, имеющих выход за границу контролируемой зоны (зоны 1).

Для проведения тестирования проверяемое СВТ размещают на поворотном столе измерительной площадки (*рис. 2*), удовлетворяющей требованиям НМД. На этом СВТ устанавливают программу СМО-ТЕСТЕР и подключают его COM-порт к выходу управления аппаратуры АРК-Д1ТИ.

Под управлением комплекса АРК-Д1ТИ начинается поочередное тестирование блоков и узлов проверяемого СВТ. Первый этап тестирования каждого из блоков СВТ направлен на выявление его информативных составляющих ПЭМИ и осуществляется при помощи программы СМО-ДХ.

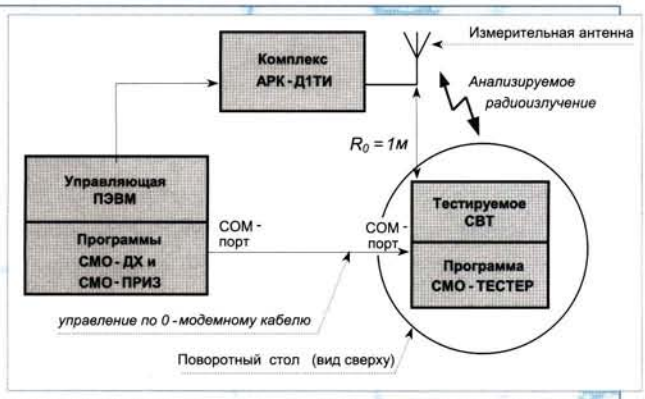

Рис. 2. Определение радиуса контролируемой зоны СВТ

Поиск информативных составляющих ПЭМИ

Поиск составляющих ПЭМИ конкретного блока СВТ производится с помощью программ СМО-ТЕСТЕР и СМО-ДХ следующим образом:

а) проверяемое СВТ при помощи программы СМО-ТЕСТЕР переводится в режим тестирования соответствующего блока. При этом используются тестовые сигналы, обеспечивающие максимальную тактовую частоту повторения информационных импульсов (пачек импульсов). Так, при тестировании мониторов ПЭВМ тестирование отображения информации следует проводить в режиме отображения вертикальных полос шириной в 1 пиксель – режим «точка через точку» или в режиме «шахматное поле» с размером элемента в 1 пиксель;

б) измерительная антенна комплекса устанавливается на минимальном расстоянии от исследуемого СВТ (источника излучения) – несколько десятков см – для наиболее эффективного обнаружения даже слабых составляющих ПЭМИ;

в) на управляющей ПЭВМ комплекса АРК-Д1ТИ запускается программа СМО-ДХ. Оператор выставляет соответствующие свойствам проверяемого блока СВТ границы тестирования по частоте и включает режим «панорама» для предварительной оценки радиообстановки. При работе в этом режиме проверяемое СВТ автоматически переводится в пассивное состояние, обеспечивающее минимальный уровень излучения проверяемого блока (например, при тестировании монитора его экран гасится), и производится накопление информации о наблюдаемых в полосе частот радиоизлучениях, не принадлежащих исследуемому блоку. Это позволяет в дальнейшем существенно сократить время поиска информативных составляющих ПЭМИ;

г) программа СМО-ДХ, управляющая комплексом АРК-Д1ТИ переводится в режим «обнаружение», в котором производится поиск составляющих ПЭМИ проверяемого блока. При этом тестируемое СВТ автоматически переключается в активный режим работы, обеспечивающий максимум излучения проверяемого блока, это позволяет выявлять компоненты ПЭМИ блока как сигналы, заметно превышающие накопленную ранее панораму радиоизлучений. Все превышающие установленный в задании пороговый уровень составляющие радиоизлучения подвергаются проверке на информативность;

д) выделение в найденной совокупности составляющих ПЭМИ информативных компонент комплекс АРК-Д1ТИ осуществляет автоматически. Для этого оценивается взаимная корреляция между переключением тестируемого СВТ в активный/пассивный режим и изменением параметров излучаемых радиосигналов. Обнаружение такой зависимости указывает, что анализируемый сигнал может представлять угрозу утечки информации. Итак, по результатам проверки информативности обнаруженные составляющие ПЭМИ разделяются на новые – не опасные обнаруженные сигналы, не имеющие информативной зависимости, и идентифицированные – радиоизлучения, модулированные информативными сигналами;

е) поиск информативных составляющих ПЭМИ завершается измерением интенсивностей найденных компонент и передачей результатов измерений в базу данных программы СМО-ПРИЗ. Окно программы СМО-ДХ при передаче результатов измерений в программу СМО-ПРИЗ показано на *рис. 3*.

Измерение интенсивности информативных составляющих ПЭМИ и передача результатов измерений программе СМО-ПРИЗ для дальнейшего анализа

Процедура измерения интенсивности составляющих ПЭМИ и передача их программе СМО-ПРИЗ включает следующие действия:

а) проверяемый блок СВТ переключается в активный (тестовый) режим работы. Для каждой из частот f_j информативных составляющих ПЭМИ за счет вращения поворотного стола и подбора положения измерительной антенны определяется направление наиболее интенсивного излучения. В найденном направлении на удалении d в 1 м от СВТ производится измерение уровня

напряженности электромагнитного поля $E_{и\,m\,j}$, излучаемого в тестовом режиме работы *m*-блоком СВТ на *j*-частоте. Результаты измерений выражаются в децибелах относительно микровольта. Линейность измерительного тракта АРК-Д1ТИ позволяет определять уровни спектральных составляющих во всем частотном диапазоне сигналов с точностью 1 – 2 дБ/мкВ;

б) проверяемый блок или тестируемое СВТ в целом выключается, и для каждой из ранее найденных частот производится измерение уровней напряженности $E_{п\,j}$, создаваемой на тех же частотах естественным электромагнитным фоном;

в) результаты измерений автоматически передаются в базу данных программы СМО-ПРИЗ. Оператору остается лишь уточнить по полученным данным тактовую частоту F_T, длительность импульсов τ_m и скважность Q_m тестового сигнала *m*-блока СВТ (о методике подобного уточнения будет сказано ниже).

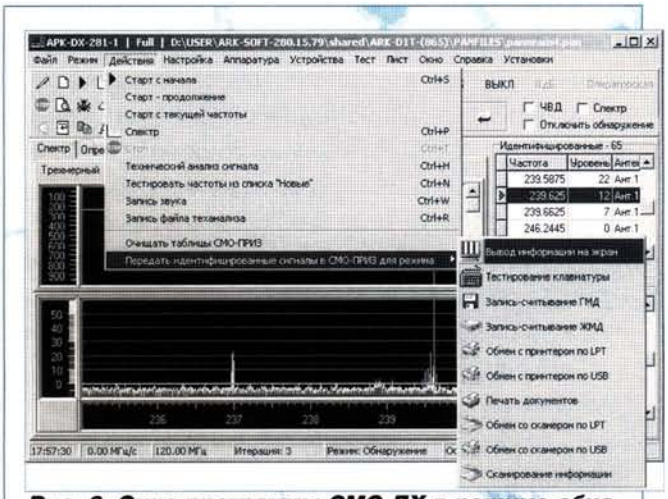

Рис. 3. Окно программы СМО-ДХ в режиме обнаружения информативности составляющих ПЭМИ и передачи результатов в программу СМО-ПРИЗ

Расчет радиуса контролируемой зоны программой СМО-ПРИЗ

Программа СМО-ПРИЗ реализует завершающий этап лабораторных исследований СВТ, осуществляя по переданным данным расчет радиуса контролируемой зоны. Структурная схема алгоритма для определения радиуса представлена на *рис. 4*. В этой схеме использованы следующие обозначения:

$E_{c\,m\,j}$ – измеряемая в микровольтах на метр напряженность сигнальной составляющей информативной компоненты ПЭМИ, излучаемой *m*-тестируемым блоком СВТ на частоте f_j, рассчитывается по измеренным уровням напряженности электромагнитного поля $E_{и\,m\,j}$ и $E_{п\,j}$ в соответствии с правилом

$$E_{c\,mj} = \sqrt{10^{0,1\,E_{и\,mj}} - 10^{0,1\,E_{nj}}}\ \text{(мКв/м)}, \qquad (8)$$

Q_m – скважность тестового сигнала *m*-блока СВТ;

$K_{oj}(r)$ – коэффициент затухания электромагнитного поля в свободном пространстве, определяемый текущими НМД;

$K_{n\,m}$ – коэффициент разрядности *m*-блока СВТ (для параллельных кодов $K_{n\,m} = n/2$, где *n* – число разрядных цепей исследуемого блока; для последовательных кодов $K_{n\,m} = 1$);

$E_{шн}(f)$ – соответствующая текущему типу средств разведки напряженность поля нормированных шумов, рассчитываемая согласно НМД;

ΔF_1 – частотный интервал, которому принадлежат тестируемые составляющие ПЭМИ, ширина которого определяется длительностью импульсов τ_m тестового сигнала проверяемого блока СВТ

$$\Delta F_i = \frac{1}{\tau_m}; \qquad (9)$$

$\delta_{норм}$ – предельно допустимое для текущей категории объектов отношение сигнал/помеха в точке возможного размещения средств перехвата информации.

Из *рис. 4* видно, что радиус R_2 контролируемой зоны определяется итеративным путем как наименьшее расстояние, на котором для всех блоков СВТ и всех частотных интервалов ΔF_i отношение сигнал/шум Δ не превышает предельно допустимое по НМД значение $\delta_{норм}$.

Рис. 4. Структурная схема алгоритма расчета радиуса контролируемой зоны R_2 при оценке защищенности СВТ от утечки информации по каналу ПЭМИ

Лабораторные исследования СВТ включают в себя также расчет радиусов зон r_1 и r_1', представляющих собой минимально допустимые расстояния от СВТ до вспомогательных технических средств и систем и их кабельных коммуникаций, имеющих выход за границу контролируемой зоны. Радиус r_1 рассчитывается по отношению к сосредоточенным, а радиус r_1' – по отношению к распределенным случайным антеннам. Расчеты этих величин производятся аналогично расчету радиуса зоны R_2, но с заменой напряженности поля нормированных шумов $E_{шн}(f)$ уровнями

чувствительности сосредоточенных и распределенных случайных антенн, задаваемыми НМД.

Примерный вид главного окна программы СМО-ПРИЗ в режиме расчета радиуса контролируемой зоны показан на *рис. 5*. Первые пять колонок таблицы, представленной в левой части окна, содержат данные измерений интенсивностей ПЭМИ. В ходе описанных выше процедур эти колонки заполняются автоматически. Последние колонки, имеющие серый фон, отображают рассчитанный в соответствии с (8) уровень сигнальной составляющей и номер интервала частот, которому принадлежит текущая компонента ПЭМИ. Таблицы, отображаемые в правой части окна, характеризуют зависимость радиуса контролируемой зоны R_2 от категории объекта информатизации, типа применяемых средств разведки (стационарные, возимые, носимые) и номера текущего частотного интервала.

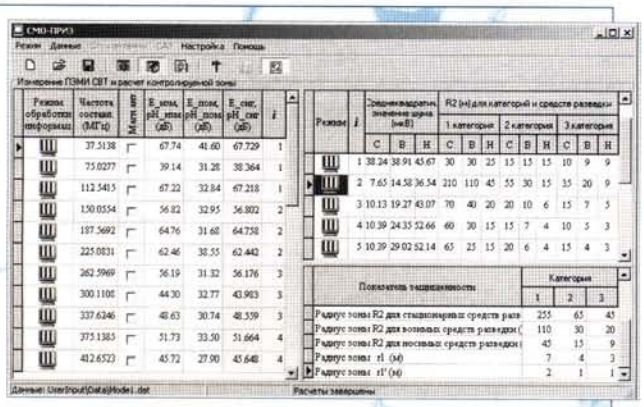

Рис. 5. Расчет радиуса контролируемой зоны

Поскольку программа СМО-ПРИЗ производит перерасчет показателей защищенности непосредственно по мере поступления сведений, то итоговое значение радиуса R_2 оказывается доступным сразу после завершения ввода данных по совокупности блоков исследуемого СВТ. В связи с этим оператор непосредственно в процессе ввода данных может контролировать изменение показателей защищенности информации, а протокол испытаний готов для распечатки сразу после завершения ввода информации.

Итак, программное обеспечение комплекса АРК-Д1ТИ обеспечивает полномасштабное исследование свойств СВТ в автоматизированном режиме. Результаты расчетов и формируемые по результатам исследований протоколы полностью соответствуют требованиям действующих в настоящее время НМД.

Уточнение параметров тестового сигнала для установленного режима работы СВТ

Полученное выше соотношение (7) предполагает наличие информации о тактовой частоте F_T и скважности Q тестового сигнала, однако на практике точные значения этих параметров неизвестны и должны уточняться по ходу исследований. Как правило, определение этих параметров производится в 2 этапа. Сначала из априорных данных о режиме тестирования рассчитывают приближенные значения параметров режима, а затем на основе измеренных интенсивностей информативных составляющих ПЭМИ уточняют эти значения. Рассмотрим определение этих параметров на примере тестирования ЖК- и ЭЛТ-мониторов.

Предварительный расчет параметров режима тестирования для ЖК-монитора

Рассмотрим случай, когда выбранная оператором частота вертикальной развертки равна $F_{вер} = 60$ Гц, а разрешение экрана составляет $P_{гор}\times P_{вер} = 1280\times1024$ пикселей. Частота горизонтальной развертки будет при этом равна $F_{стр} = P_{вер}\cdot F_{вер} = 1024\cdot60 \approx 60$ кГц. В режимах отображения «точка через точку» число темных вертикальных линий (темных квадратиков шахматного поля в каждой строке изображения) будет равно $m = P_{гор} / 2 = 1280/2 = 640$. В результате возникает периодическая последовательность элементов отображения с тактовой частотой $F_T = m\cdot F_{стр} = 640\cdot60 = 38400$ кГц $= 38{,}4$ МГц.

В ЖК-мониторе форма видеосигнала соответствует формируемому изображению и в рассматриваемом случае представляет собой последовательность со скважностью $Q = 2$. Таким образом, $\tau = 1/\Delta F = 1/(Q\times F_T) = 1/76{,}8$ МГц $= 0{,}013$ мкс.

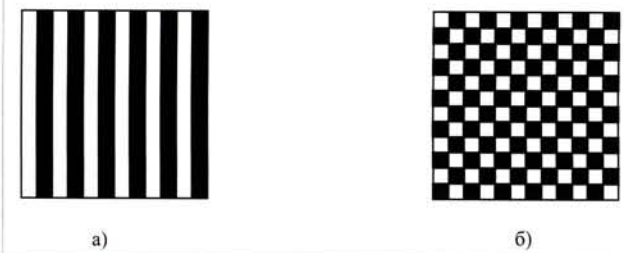

Рис. 6а. Изображение при активном состояния режима «вертикальные линии»
Рис. 6б. Изображение при активном состоянии режима «шахматное поле»

Предварительный расчет параметров режима тестирования для ЭЛТ-монитора

Пусть ЭЛТ-монитор работает в режиме с разрешением $P_{гор}\times P_{вер} = 1024\times768$ пикселей и частотой вертикальной развертки $F_{вер} = 70$ Гц. Частота горизонтальной развертки при этом будет равна $F_{стр} = P_{вер}\times F_{вер} = 768\times70 \approx 54$ кГц. При отображении вертикальных линий или шахматного поля с размером элементов в 1 пиксель каждая строка будет содержать $m = P_{гор} / 2 = 1024/2 = 512$ периодов элементов отображения и тактовая частота формируемой последовательности импульсов составит $F_T = m\times F_{стр} = 512\times54 = 27640$ кГц $= 27{,}64$ МГц.

Определение длительности формируемых импульсов для сигналов ЭЛТ-монитора может представлять определенную проблему, т.к. для повышения четкости изображения

импульсы видеосигнала имеют меньшую длительность, чем «длительность» отображаемых пикселей. Вследствие этого скважность формируемой последовательности импульсов оказывается превышающей 2 и должна определяться непосредственно по результатам спектральных исследований, а длительность импульса оказывается меньше таковой для ЖК-монитора:

$\tau < 1/\Delta F = 1/(Q \times F_T) = 1/55{,}28$ МГц $= 0{,}0181$ мкс.

Уточнение длительности импульса тестового сигнала для ЭЛТ-монитора

Уточнение параметров режима тестирования ЭЛТ-монитора производится в 2 этапа.

На первом по выявленной в результате радиоизмерений периодичности размещения составляющих ПЭМИН на оси частот уточняется значение тактовой частоты F_T.

На втором этапе, также по результатам радиоизмерений, определяется частота f_r ближайшей гармоники тактовой частоты, принимающей нулевое значение, и методом перебора определяется простое число $\nu \in \{2, 3, 5, 7, 11, 13\}$, для которого выполняется условие:

$$3F_T \leqslant f_r/\nu \leqslant 4F_T. \quad (10)$$

В этом случае

$$\tau = \nu/f_r, \quad (11)$$

$$1/\tau = f_r/\nu, \quad (12)$$

а скважность $Q = f_r/(\nu \times F_T)$.

Если подбором ν условие (10) выполнить не удается, то подбор следует повторить, ориентируясь на альтернативное условие

$$2 \times F_T < \frac{f_r}{\nu} \leq 4 \times F_T. \quad (13)$$

Значения параметров тестирования, получаемые по данной методике, служат основой расчетов показателей защищенности информации, осуществляемой программой СМО-ПРИЗ.

Решение задач контроля защищенности информации на объектах информатизации

Выше уже говорилось, что программа СМО-ПРИЗ обеспечивает расчет всех показателей защищенности информации, предусматриваемых требованиями НМД. Пример ее использования для определения радиуса контролируемой зоны был приведен в предыдущих разделах. Теперь коротко остановимся на решении других задач информационной защищенности.

Целью как аттестационных испытаний, так и оценки эффективности принятых мер защиты информации является установление в соответствии с НМД уровня побочных электромагнитных излучений и наводок на границе контролируемой зоны объекта информатизации. Защищенность информации от утечки по каналу ПЭМИН считается удовлетворительной, если все полученные при анализе блоков СВТ отношения сигнал/шум не превышают предельной величины, соответствующей категории проверяемого объекта информатизации. Все исследования защищенности информации на объектах информатизации реально производятся по алгоритму, структурная схема которого показана на *рис. 7*. Отличия заключаются лишь в деталях расчетов показателей информационной защищенности.

Рис. 7. Структурная схема алгоритма оценки защищенности информации, обрабатываемой СВТ

Особенность проведения аттестационных испытаний

Особенностью аттестационных испытаний является их проведение непосредственно на объекте информатизации и необходимость учета особенностей его расположения по отношению к потенциальным местам размещения средств разведки, реально наблюдаемых затуханий сигналов при распространении ЭМП к границе контролируемой зоны и т.п. Теоретический учет таких особенностей оказывается весьма сложным и недостаточно точным [3]. С учетом этого расчет показателей защищенности при аттестационных испытаниях производят с определением и использованием коэффициентов реального затухания сигналов

$$K_{pj} = \begin{cases} E_{dj}/E_{Ruj} & при\ R_u = R, \\ \dfrac{E_{dj}K_{oj}(R)}{E_{Ruj}K_{oj}(R_u)} & при\ R_u < R, \end{cases} \quad (14)$$

где E_{dj} – соответствующая частоте f_j напряженность поля сигнала, сформированного вспомогательным генератором вблизи СВТ; E_{Ruj} – напряженность поля, измеренная на расстоянии R_u от СВТ; R – расстояние до места возможного размещения средств разведки.

Показатели защищенности информации

При оценке защищенности информации от утечки по каналу ПЭМИ расчет показателя информационной защищенности выполняется в соответствии с выражением

$$\Delta_m = \max_i \left\{ \sqrt{\frac{Q_m}{2} \times \sum_j \left(\frac{E_{c\,mj}}{K_{pj}} \right)^2} \Bigg/ K_{nm} \times \sqrt{\int_{\Delta F_i} \left(E_{шн}(f)\right)^2 df} \right\}, \quad (15)$$

где, $E_{c\,m\,j}$ – измеряемая в микровольтах на метр напряженность сигнальной составляющей ПЭМИ, излучаемой тестируемым m-блоком СВТ на частоте f_j, рассчитываемая согла-

сно (8); Q_m – скважность тестового сигнала для m-блока СВТ; $K_{n\,m}$ – его коэффициент разрядности; $E_{шн}(f)$ – соответствующая текущему типу средств разведки напряженность поля нормированных шумов; ΔF_i – частотный интервал (9), которому принадлежат тестируемые составляющие ПЭМИ.

При исследовании опасности утечки информации за счет наводок расчет интенсивности сигнальных составляющих наведенных напряжений производится по правилу

$$U_{c\,m\,j} = \sqrt{U_{и\,m\,j}^2 - U_{п\,m\,j}^2}\ \text{(мкВ)}, \qquad (16)$$

где $U_{и\,m\,j}$ – напряжение, наводимое в тестируемой линии на частоте f_j при работе m-блока СВТ в активном режиме; $U_{п\,j}$ – напряжение, создаваемое в той же линии естественным электромагнитным фоном при выключенном СВТ. Правило расчета показателя информационной защищенности приобретает вид

$$\Delta_m = \max_i \left\{ \sqrt{\frac{Q_m}{2} \times \sum_j \left(\frac{U_{c\,m\,j}}{K_{лj}} \right)^2} \Bigg/ K_{n\,m} \times \sqrt{\int_{\Delta F_i} \left(h_д(f) \times E_{шн}(f) \right)^2 df} \right\}, \qquad (17)$$

где $K_{л\,j}$ – реальный коэффициент затухания сигналов в тестируемой линии, действующая высота $h_д(f)$ характеризует свойства тестируемой линии в качестве случайной антенны (эта зависимость аппроксимируется по результатам измерений), а параметры Q_m, $E_{шн}(f)$ и ΔF_i остаются теми же, что и при анализе канала ПЭМИ.

В случаях когда для улучшения защиты информации на объекте информатизации используется система активного зашумления (САЗ), при расчете показателя защищенности вместо нормативной интенсивности шума используется реально создаваемая системой САЗ напряженность поля помехи. В результате правило (7) приобретает вид

$$\Delta_m = \max_i \left\{ \sqrt{\frac{Q_m}{2} \times \sum_j \left(\frac{E_{c\,m\,j}}{K_{рj}} \right)^2} \Bigg/ K_ш \times K_{n\,m} \times \sqrt{\sum_k \left(\frac{E_{ш\,k}}{K_{рш\,k}} \right)^2} \right\}, \qquad (18)$$

где $E_{ш\,k}$ – значение напряженности поля шума, создаваемого САЗ на k-частоте; $K_{рш\,k}$ – коэффициент реального затухания шума, создаваемого генератором САЗ; $K_ш$ – коэффициент качества шума САЗ. Прочие параметры, включая правило (8) расчета напряженности $E_{c\,m\,j}$ сигнальной составляющей ПЭМИ, полностью соответствуют ранее разобранным случаям.

Наконец, при оценке эффективности принятых мер защиты информации применительно к каналу наводок упомянутое в алгоритме на *рис. 7* правило расчета показателя информационной защищенности приобретает вид

$$\Delta_m = \max_i \left\{ \sqrt{\frac{Q_m}{2} \times \sum_j \left(\frac{U_{c\,m\,j}}{K_{лj}} \right)^2} \Bigg/ K_ш \times K_{n\,m} \times \sqrt{\sum_k U_{шc\,k}^2} \right\}, \qquad (19)$$

где $U_{шc\,k}$ – среднеквадратическое значение напряжения шума, создаваемого в линии генератором САЗ на k-частоте, расчет интенсивности информативных составляющих наведенных сигналов производится по правилу (16), а все прочие обозначения соответствуют ранее разобранным случаям.

Работа программы СМО-ПРИЗ при контроле защищенности информации

На *рис. 8 – 9* приведены окна программы СМО-ПРИЗ для режима контроля защищенности информации в случаях использования на объекте информатизации системы САЗ и без нее.

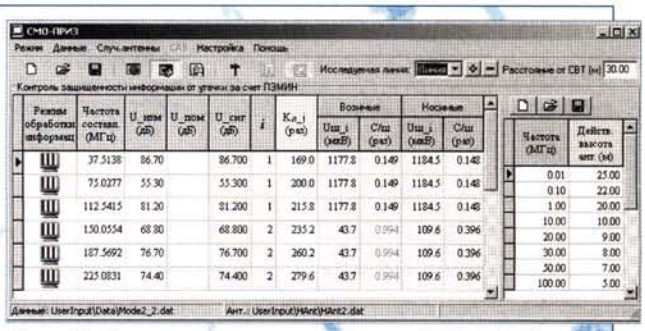

Рис. 8. Главное окно программы СМО-ПРИЗ при анализе защищенности информации от утечки по каналу наводок (в отсутствие системы САЗ)

Начальные колонки таблицы, представленной в левой части окна, содержат результаты измерений интенсивности выявленных информативных составляющих ПЭМИ. Поскольку пример на *рис. 8* иллюстрирует анализ наводок, то информация об интенсивности наведенных сигналов теперь представлена измеренными напряжениями, а тестируемая линия характеризуется действующей высотой антенны и коэффициентом затухания – едиными для всех типов средств разведки. Предназначенные для их ввода колонки «действ. высота антенны (м)» и «Кл_j (раз)» имеют подсвеченные заголовки и позволяют не только непосредственно вводить значения, но и использовать для их получения встроенные расчетные формы.

Колонки таблицы, имеющие голубоватый фон, отображают рассчитанный в соответствии с (16) уровень сигнальной составляющей, номер интервала частот, которому принадлежит текущая компонента ПЭМИ, в колонках «С/ш (раз)» – отношение сигнал/помеха на границе контролируемой зоны, рассчитанное для этих интервалов частот. Тот факт, что ряд значений в представленной на *рис. 8* таблице выделен красным цветом, указывает на нарушение требований норм защищенности информации в соответствующих интервалах частот.

Работа СМО-ПРИЗ в режиме оценки эффективности принятых мер защиты информации (*рис. 9*) во многом похожа на ее работу при оценке защищенности информации и отличается лишь дополнительным учетом данных, характеризующих работу системы защиты. Эти данные отображаются в правой части главного окна СМО-ПРИЗ. Дополнительная панель инструментов, расположенная непосредственно над таблицей данных о системе САЗ, и раздел «САЗ» глав-

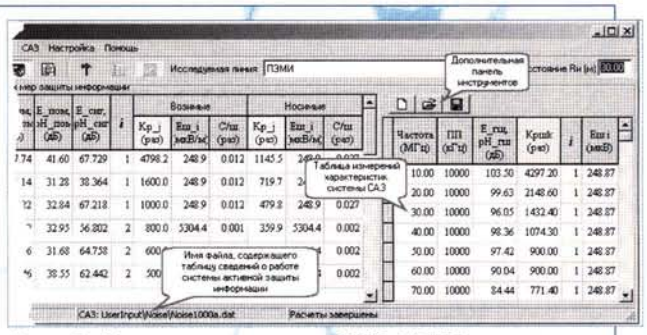

Рис. 9. Вид главного окна СМО-ПРИЗ при оценке эффективности принятых мер защиты информации (при действии системы САЗ)

ного меню программы позволяют сохранять характеристики САЗ на диске и подключать к расчету ранее сохраненные (или созданные внешними приложениями) таблицы.

Пример, приведенный на *рис. 9*, показывает, что применение системы зашумления позволяет обеспечить существенно меньшие значения наблюдаемого соотношения сигнал/помеха (содержимое колонок «С/ш (раз)»). Тем самым обеспечивается надежное выполнение требований норм защищенности информации во всех интервалах частот.

Еще раз отметим, что программа СМО-ПРИЗ вычисляет показатели информационной защищенности непосредственно по ходу получения данных, оператор имеет полный контроль над ходом расчетов, а протокол испытаний оказывается доступным для распечатки сразу после завершения ввода информации.

Совместная работа программы СМО-ПРИЗ с другими средствами измерений

При необходимости программа расчета информационной защищенности СМО-ПРИЗ может использоваться совместно не только с комплексом АРК-Д1ТИ, но и с другими средствами радиоизмерений. Для автоматизации передачи результатов измерений в составе пакета СМО-ПРИЗ имеется специальный модуль, предназначенный для преобразования данных от внешнего приложения в формат базы данных СМО-ПРИЗ. Это делает возможным передавать данные измерений в программу СМО-ПРИЗ из других программ, отличных от СМО-ДХ.

Заключение

Многофункциональный комплекс радиомониторинга АРК-Д1ТИ является современным сертифицированным средством радиоизмерений, позволяющим эффективно решать задачи оценки защищенности информации от утечки по каналу ПЭМИН.

При исследовании опасности утечки информации по каналу ПЭМИН комплекс АРК-Д1ТИ обеспечивает обнаружение компонент ПЭМИ проверяемого оборудования, автоматически выявляя информативные составляющие излучений, производит измерения их интенсивности и рассчитывает показатели защищенности информации. Подобная автоматизация позволяет сократить время проведения испытаний, облегчить работу оператора и обеспечить принятие объективных решений о степени защищенности информации. Комплекс АРК-Д1ТИ имеет небольшие габариты, массу, может использоваться как в стационарном, так и в подвижном варианте в качестве носимого или возимого средства.

Обновленное в 2005 г. программное обеспечение комплекса включает модифицированную версию программы проведения анализа электромагнитной обстановки СМО-ДХ и специализированную программу расчета информационной защищенности СМО-ПРИЗ, позволяющую выполнять расчеты радиуса контролируемой зоны для средств вычислительной техники, показателей защищенности информации от утечки по каналам ПЭМИН и оценки эффективности принятых мер защиты информации. Программа СМО-ПРИЗ сертифицирована, прошла апробацию и полностью соответствует требованиям НМД, действующим с 2005 г.

В настоящее время продолжаются разработки, направленные на совершенствование аппаратуры радиоконтроля в направлении защиты информации от утечки по каналу ПЭМИН. В 2006 г. планируется выпуск нового специализированного программного обеспечения СМО-ТЕЗИС, отличительными особенностями которого будет использование новых методов выявления информативных составляющих.

Литература

1. *Бурмин В.А., Быковников В.В., Тупота В.И. Многофункциональный комплекс контроля эффективности защиты информации АРК-Д1ТИ / Специальная техника, 2002, Спец. выпуск, с. 49 – 56.*
2. *Кузнецов Ю.В., Баев А.Б. Методы измерения ПЭМИН: сравнительный анализ/ Конфидент, 2002, № 4, 5, с. 54 – 57.*
3. *Бурмин В.А., Быковников В.В., Новиков А.В., Тупота В.И. Применение программно-аппаратного комплекса АРК-Д1ТИ для решения задачи оценки информационной защищенности/ Специальная техника, 2003, Спец. выпуск, с. 60 – 64.*
4. *Каталог компании «ИРКОС», Москва, 2006.*
5. *АРК-Д1ТИ – комплекс радиомониторинга многофункциональный портативный. Сертификат Госстандарта РФ об утверждении типа средств измерений RU.E.35.018.A № 18190 от 04.07.2004, зарегистрирован в Государственном реестре средств измерений под № 27326-04.*
6. *АРК-Д1ТИ – многофункциональный портативный комплекс радиомониторинга и выявления технических каналов утечки информации. Сертификат ФСТЭК № 506/1 от 01.02.2005.*
7. *АРК-КНВ4 – конвертер выносной. Сертификат Госстандарта России об утверждении типа средств измерений RU.E.33.018.A № 17735 от 04.06.2004, зарегистрирован в Государственном реестре средств измерений под № 26994-04.*
8. *СМО-ПРИЗ – программа расчета параметров защищенности технических средств обработки информации по требованиям безопасности информации. Сертификат ФСТЭК № 1102 от 28.11.2005.*