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

ОБНАРУЖЕНИЕ И ОЦЕНКА ИНФОРМАТИВНОСТИ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Побочными электромагнитными излучениями (ПЭМИ) называют паразитные электромагнитные поля, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными. Существование ПЭМИ может приводить к утечке конфиденциальной информации при ее передаче или обработке. Действительно, если характеристики поля, распространяющегося вокруг устройства обработки, взаимосвязаны с обрабатываемой информацией, то, анализируя характер изменения электромагнитного поля чувствительным радиоприемником, можно перехватить информацию на значительном расстоянии. В связи с этим устройства, применяемые для обработки конфиденциальной информации, подвергают специальным исследованиям, целью которых является выявление и анализ интенсивности создаваемых ими информативных ПЭМИ.

В работе [1] рассматривалось применение сертифицированного комплекса радиомониторинга АРК-Д1ТИ [2, 3] для тестирования защищенности информации, обрабатываемой средствами вычислительной техники (СВТ), от утечки по каналу ПЭМИ. Вместе с тем методика поиска информативных составляющих, приведенная в [1], не является единственно возможной. Рассмотрим альтернативный метод, который позволяет выявлять информативные составляющие ПЭМИ с меньшими затратами времени. Для выяснения отличительных особенностей нового метода кратко рассмотрим типовую методику поиска информативных составляющих.

Типовая методика выявления информативных составляющих ПЭМИ

Выявление информативных составляющих производится в два этапа. Первый этап базируется на сравнении усредненных периодограмм. Сначала в контролируемом диапазоне частот производят усреднение наблюдаемых спектральных оценок при пассивном режиме работы тестируемой аппаратуры. Затем накопление спектральных данных повторяют, переключив проверяемое оборудование в активный (тестовый) режим. В результате сопоставления полученных периодограмм формируется список частот составляющих ПЭМИ, подлежащих проверке на информативность. Отметим, что для предотвращения пропусков слабых составляющих ПЭМИ на первом этапе приходится использовать низкий порог обнаружения, чтобы зафиксировать даже малые, в один-два децибела изменения амплитуд спектров в пассивном и тестовом режиме. Вместе с тем низкий порог обнаружения неизбежно приводит к существенному возрастанию количества

«подозрительных» частот, заносимых в список проверки на информативность.

Целью второго этапа является проверка информативности всех «подозрительных» частот из сформированного списка. Эта проверка может осуществляться оператором «на слух» с использованием того или иного набора демодуляторов или автоматически за счет поочередной узкополосной обработки входящих в список составляющих ПЭМИ. Критерием информативности служит выявление взаимосвязи между режимом работы тестируемого устройства и наблюдаемым распределением по частотам мощности спектральных составляющих. Результативность второго этапа зависит от набора демодуляторов, применяемых для перехода к узкополосной обработке, причем угадать заранее, какой именно демодулятор окажется наиболее эффективным, весьма проблематично. Для повышения достоверности желательно использовать все имеющиеся демодуляторы и подробно (на протяжении многих циклов) проверять наличие или отсутствие взаимосвязи между режимом работы тестируемого устройства и наблюдаемым распределением мощности для выходного сигнала каждого из демодуляторов. Отметим, что использование в типовой методике набора демодуляторов, по всей видимости, идет от ручного режима, при котором оператор проверяет информативность составляющих «на слух» – по изменению тональности демодулированного сигнала, происходящему синхронно с переключением тестируемой аппаратуры.

Практическое использование рассмотренной методики сопровождается существенными временными затратами, поскольку каждая частота, внесенная в список, тестируется отдельно от остальных с использованием всего набора демодуляторов. Надо отметить, что для аппаратуры радиомониторинга с низким спектральным разрешением (более 1 кГц) подобная методика оказывается, по-видимому, единственно возможной. Однако, если комплекс радиомониторинга обеспечивает высокую разрешающую способность по частоте, то применение демодуляторов не является принципиально необходимым, так как изменение распределения мощности спектральных составляющих ПЭМИ может быть обнаружено непосредственно по спектру в широкой полосе частот. Это позволяет одновременно обнаруживать и проверять информативность составляющих ПЭМИ, попадающих в полосу спектрального анализа. Чтобы разобраться в сути предлагаемого метода, который в дальнейшем будем называть методом ТОС (тестирование и обнаружение совместное), остановимся на свойствах спектральных оценок.

Вероятностные характеристики периодограммных отсчетов

Первичными данными, доступными для анализа в системе радиомониторинга, являются временные выборки наблюдаемых сигналов $s_r(k)$, где r – порядковый номер выборки, k – номер отсчета в выборке ($0 \leqslant k \leqslant N-1$, N – объем выборки). Каждую выборку можно разложить на спектральные составляющие, используя дискретное преобразование Фурье (ДПФ)

$$\dot{c}_r(n) = \frac{1}{N}\sum_{k=0}^{N-1} s_r(k) \times exp\left(-j2\pi\frac{nk}{N}\right),\ 0 \leqslant n \leqslant N-1. \quad (1)$$

Случайный характер анализируемых сигналов препятствует объединению комплексных спектров (1), полученных по разным выборкам, т.к. они отличаются друг от друга случайными фазовыми поправками. Вместе с тем модули отсчетов спектра (1) характеризуются существенной дисперсией, а потому в задачах, требующих стабильности исходных данных, вместо них используют усредненную периодограмму

$$X(n) = \sqrt{\frac{1}{R} \times \sum_{r=1}^{R} \left|\dot{c}_r(n)\right|^2}. \quad (2)$$

Там же, где устойчивость исходных данных не является критичной, могут использоваться и неусредненные периодограммы

$$X_r(n) = \left|\dot{c}_r(n)\right|. \quad (3)$$

Анализ статистических свойств отсчетов спектров реально наблюдаемых ПЭМИ СВТ показал, что интенсивность информативных составляющих ПЭМИ может быть достаточно точно аппроксимирована нормальным распределением

$$W(x;n) \approx \frac{1}{\sqrt{2\pi} \times \sigma_n}\ exp\left[-\frac{1}{2\sigma_n^2} \times (x - a_n)^2\right], \quad (4)$$

где a_n – параметр, характеризующий интенсивность сигнальной компоненты на n-ой частоте, b_n – среднеквадратическое отклонение, определяющее для того же отсчета интенсивность шумовой компоненты.

При проверке оборудования параметр a_n для информативных ПЭМИ будет меняться при смене пассивного режима тестовым. Для неинформативных ПЭМИ этот параметр остается постоянным. Для отсчетов, не содержащих сигнальной компоненты, приближение (4) оказывается неточным, однако это не критично для поиска информативных составляющих.

Нормализация отсчетов периодограмм обусловлена следующим:

- побочные излучения имеют небольшую интенсивность, поэтому при их поиске приемную антенну системы радиомониторинга стараются расположить максимально близко к проверяемой аппаратуре; наблюдаемое электромагнитное поле оказывается результатом одновременного действия всех блоков (составных частей) СВТ и имеет весьма сложную структуру;
- предельно достижимое разрешение по частоте ограничивается максимально допустимым временем анализа и техническими возможностями используемой аппаратуры; типичное спектральное разрешение составляет от сотен герц до нескольких килогерц на отсчет, поэтому каждый из отсчетов периодограмм реально отражает усредненную интенсивность нескольких близко расположенных узкополосных компонент.

Совместное обнаружение и тестирование информативности составляющих ПЭМИ. Алгоритм ТОС

Пусть за счет последовательного переключения проверяемого блока СВТ из активного в пассивное состояние и обратно удалось накопить R_y периодограмм, соответствующих активному (тестовому) режиму, и R_z периодограмм, соответствующих пассивному режиму. Так как периодичность сигналов в тестовых режимах обеспечивает концентрацию сигналов ПЭМИ в узких спектральных полосах [1], а отсчеты периодограмм являются слабокоррелированными по частоте, то для выявления информативных составляющих ПЭМИ будем анализировать отсчеты разных частот отдельно друг от друга. Из значений n-го отсчета, полученных в разных периодограммах для тестового режима работы проверяемой аппаратуры, сформируем вектор $\vec{y}=\{y_1(n), y_2(n)...y_{R_y}(n)\}$; аналогичные значения, полученные при пассивном режиме работы проверяемой аппаратуры, объединим в вектор $\vec{z}=\{z_1(n), z_2(n)...z_{R_z}(n)\}$.

Если на частоте n-го отсчета нет информативной составляющей ПЭМИ (гипотеза H_0), то отсчеты векторов $\vec{y}$ и $\vec{z}$ должны подчиняться одному и тому же распределению (4) с параметрами a_{n0} и σ_{n0}. Если же справедлива гипотеза H_1 об информативности составляющей ПЭМИ на частоте n-го отсчета, то параметры a_{ny}, σ_{n1} распределения вектора $\vec{y}$ и параметры a_{nz}, σ_{n1} распределения вектора $\vec{z}$ будут отличаться друг от друга. Таким образом, функции правдоподобия приобретают вид

$$L_0(\vec{y},\vec{z})=\frac{1}{\left(\sqrt{2\pi}\times\sigma_{n0}\right)^{R_y+R_z}}\times exp\left[-\frac{1}{2\sigma_{n0}^2}\times\left(\sum_{r=1}^{R_y}\left(y_r(n)-a_{n0}\right)^2+\sum_{r=1}^{R_z}\left(z_r(n)-a_{n0}\right)^2\right)\right], \quad (5)$$

$$L_1(\vec{y},\vec{z})=\frac{1}{\left(\sqrt{2\pi}\times\sigma_{n1}\right)^{R_y+R_z}}\times exp\left[-\frac{1}{2\sigma_{n1}^2}\times\left(\sum_{r=1}^{R_y}\left(y_r(n)-a_{ny}\right)^2+\sum_{r=1}^{R_z}\left(z_r(n)-a_{nz}\right)^2\right)\right]. \quad (6)$$

При замене входящих в эти функции неизвестных параметров их максимально правдоподобными оценками отношение правдоподобия гипотез H_1 и H_0 можно преобразовать к виду

$$l(\vec{y},\vec{z})=\frac{L_1(\vec{y},\vec{z})}{L_0(\vec{y},\vec{z})}=\left(\frac{\sigma_{n0}^*}{\sigma_{n1}^*}\right)^{R_y+R_z}, \quad (7)$$

где σ^*_{n0} и σ^*_{n1} – максимально правдоподобные оценки среднеквадратических отклонений распределений.

В итоге оптимальный по критерию максимального правдоподобия алгоритм принятия решения об информативности составляющей на частоте n-го отсчета наблюдаемых периодограмм предполагает сопоставление с порогом принятия решения статистики

$$Q_{yz}(n)=\frac{\sum_{r=1}^{R_y}y_r^2(n)+\sum_{r=1}^{R_z}z_r^2(n)-\frac{1}{R_y+R_z}\times\left(\sum_{r=1}^{R_y}y_r(n)+\sum_{r=1}^{R_z}z_r(n)\right)^2}{\left(\sum_{r=1}^{R_y}y_r^2(n)-\frac{1}{R_y}\left(\sum_{r=1}^{R_y}y_r(n)\right)^2\right)+\left(\sum_{r=1}^{R_z}z_r^2(n)-\frac{1}{R_z}\left(\sum_{r=1}^{R_z}z_r(n)\right)^2\right)}\quad\begin{Bmatrix}>\Pi\rightarrow H_1\\<\Pi\rightarrow H_0\end{Bmatrix}, \quad (8)$$

где Π – выбранный порог принятия решения.

Использование статистики (8) позволяет на основе набора периодограмм с высоким разрешением по частоте выявлять для проверяемого блока СВТ одновременно все информативные ПЭМИ, наблюдаемые в некотором диапазоне (полосе одновременного спектрального анализа). Это обеспечивает выигрыш в скорости анализа защищенности информации, обрабатываемой СВТ, по сравнению с обычным подходом, отдельно проверяющим информативность каждой «подозрительной» составляющей ПЭМИ.

Порог принятия решения. Качество алгоритма ТОС

Выразить аналитически свойства статистики (8) сложно, но проведенное физическое моделирование показало, что порог принятия решения *П* можно рассчитывать по следующей эмпирической формуле

$$\hat{\Pi} = K_1 + \frac{K_2}{R - K_3}, \qquad (9)$$

где коэффициенты $K_1 \ldots K_3$ определяются требуемой вероятностью ложного обнаружения и числом отсчетов в периодограмме. В частности, при полосе одновременного анализа в 2 МГц и интервале между отсчетами 3,125 кГц рекомендуемые значения коэффициентов равны $K_1 = 1{,}02$; $K_2 = 13$; $K_3 = 3$. Если же используется более высокое разрешение по частоте (интервал между отсчетами 390 Гц), то рекомендуемые значения коэффициентов равны $K_1 = 1{,}02$; $K_2 = 9$; $K_3 = 6$.

Практическое применение алгоритма ТОС показало, что надежность выявления информативных составляющих зависит от количества обрабатываемых периодограмм, их разрешения по частоте и интенсивности обнаруживаемых составляющих ПЭМИ. Для надежного выявления информативных составляющих ПЭМИ количество периодограмм, накапливаемых в каждой контролируемой полосе частот, должно составлять несколько десятков (не менее 20 периодограмм). При этом желательно обеспечить разрешение периодограмм по частоте не хуже нескольких сотен герц; использование сравнительно небольшого числа периодограмм с высоким разрешением по частоте дает лучшие результаты, чем накопление многих периодограмм с низким спектральным разрешением. Конкретные зависимости, характеризующие метод ТОС, приведены на *рис. 1, 2*. На *рис. 1* применительно к разному разрешению по частоте Δf показаны зависимости вероятности выявления информативных составляющих ПЭМИ от количества накапливаемых и обрабатываемых широкополосных периодограмм. Параметр Δ характеризует интенсивность обнаруживаемых составляющих ПЭМИ; численно он определяется разностью выраженных в децибелах значений периодограммных отсчетов, регистрируемых при наличии и в отсутствие выявляемой компоненты ПЭМИ. Зависимости на *рис. 2* позволяют сопоставить качество выявления информативных составляющих ПЭМИ при использовании метода ТОС и типовой методики.

Рекомендованные выше пороги обнаружения обеспечивают близкую к единице вероятность обнаружения информативных составляющих ПЭМИ, в присутствии которых превышение над панорамой Δ составляет 5 и более децибел. Более слабые составляющие ПЭМИ также обнаруживаются, но, естественно, с меньшей вероятностью. За счет накопления и использования дополнительных периодограмм эту вероятность можно повысить, однако значительно эффективнее использовать периодограммы с повышенным разрешением по частоте. При использовании высокого разрешения на долю каждого отсчета периодограммы приходится гораздо меньшая доля мощности

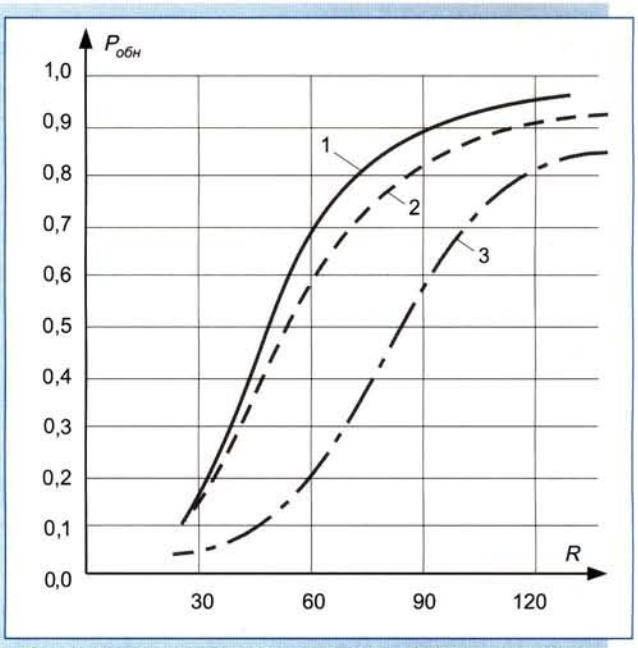

Рис. 1. Вероятность выявления информативных составляющих ПЭМИ для метода ТОС:
1 – Δ = 0 дБ, Δf = 390 Гц; 2 – Δ = 4 дБ, Δf = 3125 Гц; 3 – Δ = 3 дБ, Δf = 3125 Гц

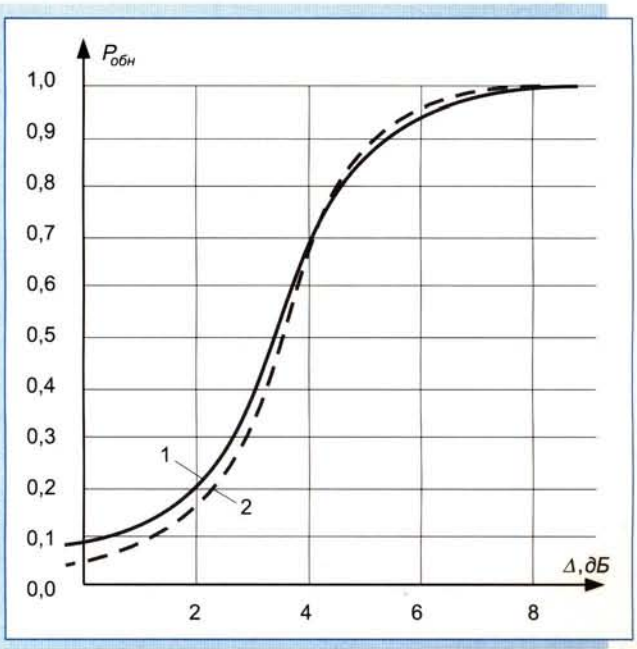

Рис. 2. Сравнение вероятностных характеристик метода ТОС и типовой методики:
1 – вероятность выявления информативных составляющих ПЭМИ для метода ТОС (R = 60, Δf = 390 Гц); 2 – вероятность выявления информативных ПЭМИ типовой методикой

шума, что позволяет обнаруживать существенно более слабые составляющие. Ценой указанного улучшения является существенное возрастание временных и аппаратных ресурсов, затрачиваемых на обработку данных.

Из *рис. 2* следует, что обеспечиваемые методом ТОС характеристики обнаружения близки к показателям типовой методики, превосходя их для слабых составляющих ПЭМИ. Вместе с тем список проверяемых частот обычно содержит десятки составляющих ПЭМИ, относящихся к одной и той же широкополосной периодограмме. При типовой методике эти составляющие тестируются поочередно, а при использовании метода ТОС – совместно друг с другом, что, как правило, позволяет в несколько раз уменьшить время, затрачиваемое на тестирование.

Программа специального математического обеспечения СМО-ТЕЗИС

Программа СМО-ТЕЗИС «Тестирование защищенности информационных систем» – это специальное математическое обеспечение, предназначенное для автоматизированного исследования защищенности информации с помощью многофункционального комплекса радиомониторинга АРК-Д1ТИ. В программе по выбору оператора используется один из четырех возможных режимов:

- автоматизированное последовательное обнаружение и тестирование информативности составляющих ПЭМИ (режим ТОР – тестирование и обнаружение раздельное);
- автоматизированное совместное обнаружение и тестирование составляющих ПЭМИ (режим ТОС);
- «ручное» обнаружение и тестирование информативности;
- расчетный режим.

На *рис. 3* показан вид окон программы в режиме ТОС.

Перед запуском автоматизированных режимов оператор должен составить задание на исследование с указанием набора проверяемых каналов утечки информации (монитор, клавиатура и т.п.), совокупности применяемых тестов и проверяемых диапазонов частот. При этом для режима ТОР требуется задавать совокупность параметров: пороги обнаружения и используемые демодуляторы, а для режима ТОС – продолжительность тестирования. Тот факт, что режим ТОР требует указания большого числа параметров обнаружения, не является его преимуществом, а, напротив, свидетельствует о его недостаточной надежности. Ошибка в выборе хотя бы одного из параметров обнаружения может заметно ухудшить итоговую эффективность работы. В режиме ТОС, напротив, увеличение продолжительности тестирования лишь повышает надежность выявления информативных составляющих ПЭМИ, а грубые ошибки в выборе оператором параметров обработки принципиально невозможны.

В дополнение к автоматизированным режимам программа СМО-ТЕЗИС предоставляет возможности «ручной» проверки получаемых данных. В любой момент оператор, приостановив автоматическое выполнение задания, имеет возможность детально исследовать заинтересовавший его участок частотной оси, переключившись в режим «Просмотр текущего спектра» или «Спектральная лупа». Дистанционно управляя состоянием тестируемой аппаратуры, он может визуально контролировать изменение текущего спектра, а также следить за характеристиками порождаемого проверяемым оборудованием радиоизлучения «на «слух». Наконец, имеется возможность формировать последовательность тестовых акустических сигналов, обеспечивая проверку наличия у проверяемой аппаратуры акустоэлектрических преобразований.

Получив данные от аппаратуры, оператор переключает программу СМО-ТЕЗИС в расчетный режим, предназначенный для вычисления показателей защищенности информации от утечки по каналу ПЭМИ. Расчет показателей производится в соответствии с изменившимися в 2005 г. нормативно-методическими документами (НМД). На *рис. 4* показаны окна программы в расчетном режиме.

Программа СМО-ТЕЗИС выполняет расчеты:

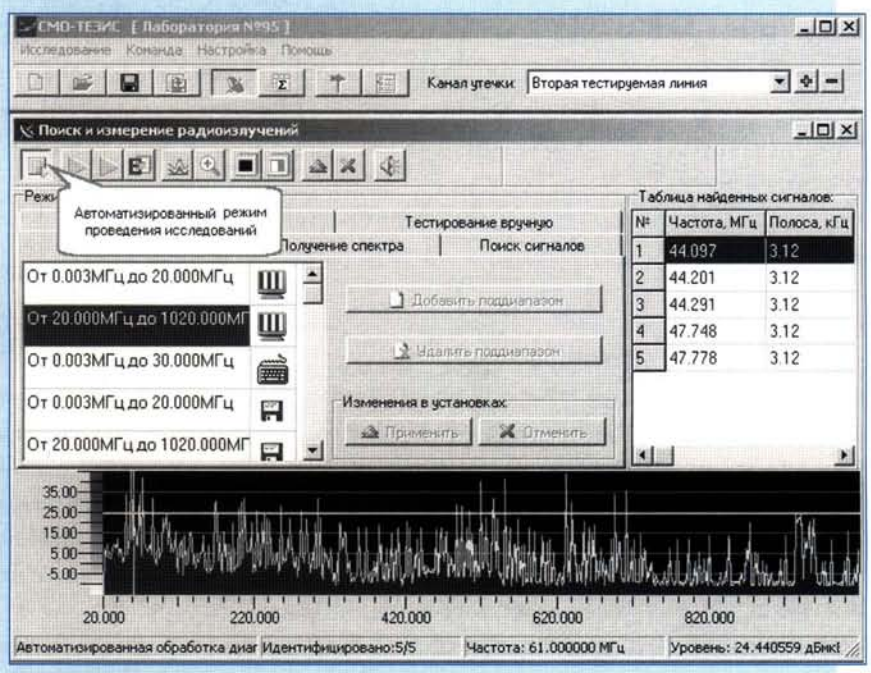

Рис. 3. Проведение исследований в автоматизированном режиме

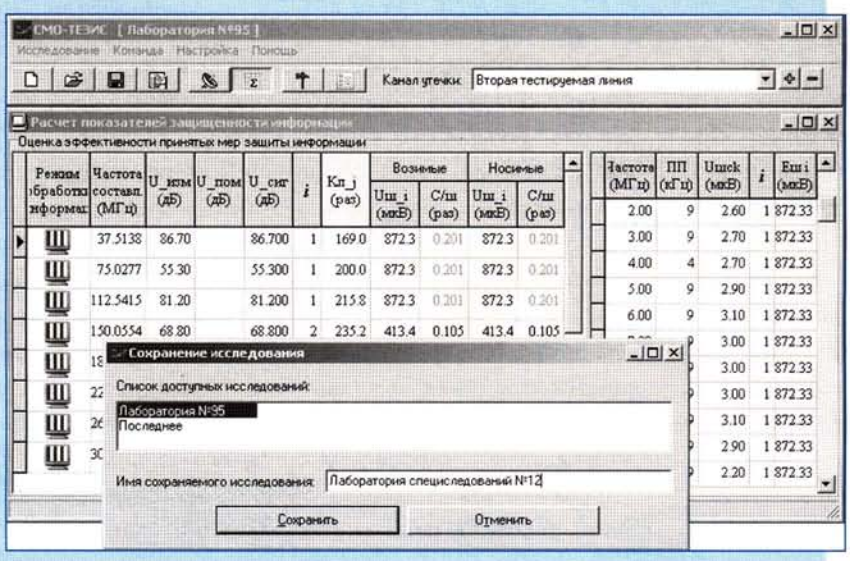

Рис. 4. Расчет показателей защищенности и сохранение результатов исследований

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

При определении радиуса контролируемой зоны для заданной совокупности тестов и указанного оператором набора частотных диапазонов СМО-ТЕЗИС:

- выявляет перечень частот информативных ПЭМИ;
- производит оценку интенсивности обнаруженных составляющих;
- рассчитывает радиусы контролируемых зон R_2, $r1$ и $r1'$, гарантирующие защиту информации от утечки по каналу ПЭМИ и каналам наводок;
- оформляет протоколы испытаний, соответствующие НМД.

При определении показателей защищенности информации на объекте информатизации программы СМО-ТЕЗИС автоматизирует измерение коэффициентов реального затухания сигналов, а также действующих высот случайных антенн. С использованием этих параметров СМО-ТЕЗИС для каждого потенциального канала утечки информации рассчитывает величину отношения сигнал/шум на границе контролируемой зоны, позволяя сопоставить реальную защищенность информации с требованиями НМД.

В ходе оценки эффективности принятых мер защиты информации программа СМО-ТЕЗИС позволяет оценивать показатели работы систем активного зашумления и рассчитывать наблюдаемую на границе контролируемой зоны величину отношения сигнал/шум.

Результаты исследований сохраняются в собственной базе СМО-ТЕЗИС. Сведения о различных тестируемых объектах хранятся независимо, что позволяет без существенных ограничений прерывать и возобновлять выполнение тестирования конкретного объекта информатизации, а также (при необходимости) использовать в работе сведения, полученные в ходе предыдущего тестирования.

Заключение

Предложенный метод ТОС для совместного обнаружения и тестирования информативности составляющих ПЭМИ имеет большее быстродействие по сравнению с типовой методикой при сохранении тех же вероятностей обнаружения информативных ПЭМИ. Для практической реализации этого метода необходима измерительная радиоаппаратура, обеспечивающая высокое, порядка сотен герц, разрешение по частоте. Примером подобной аппаратуры служит многофункциональный комплекс радиомониторинга АРК-Д1ТИ.

Метод ТОС реализован в программе СМО-ТЕЗИС, представляющей собой специализированное математическое обеспечение комплекса АРК-Д1ТИ для определения показателей защищенности информации, обрабатываемой средствами вычислительной техники. Особенностями программы являются высокая степень автоматизации, повышенное быстродействие и соответствие определяемых показателей защищенности информации требованиям современной нормативно-методической документации.

Литература

1. *Тупота В.И., Козьмин В.А., Токарев А.Б. Применение многофункционального комплекса АРК-Д1ТИ для оценивания защищенности информации от утечки по каналу ПЭМИН // Специальная техника, 2006, № 1, с. 38 – 46.*
2. *АРК-Д1ТИ – Многофункциональный портативный комплекс радиомониторинга. Сертификат Госстандарта РФ об утверждении типа средств измерений RU.C.35.002.A № 13618 от 03.12.2002, зарегистрирован в Государственном реестре средств измерений под № 23924-02.*
3. *АРК-Д1ТИ – Многофункциональный портативный комплекс радиомониторинга и выявления технических каналов утечки информации. Сертификат ФСТЭК № 506/1 от 01.02.2005.*