

**ТУПОТА Виктор Иванович,
доктор технических наук, профессор
КОЗЬМИН Владимир Алексеевич,
кандидат технических наук, доцент
ПЕРЕВЕРЗЕВ Сергей Борисович
ПЕТИГИН Алексей Федорович
ТОКАРЕВ Антон Борисович,
кандидат технических наук, доцент**

АВТОМАТИЗАЦИЯ ИССЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПЭМИН

Aппаратура для исследования побочных электромагнитных излучений и наводок

Электромагнитные поля, возникающие как побочный продукт работы устройств обработки информации, и вызываемые этими полями наведенные напряжения называют побочными электромагнитными излучениями и наводками (ПЭМИН). Задача анализа опасности ПЭМИН с позиций возможности утечки информации является весьма сложной и трудоемкой. Для ее эффективного решения используют автоматизированные комплексы радиомониторинга, выпускаемые разными производителями.

В основе работы всех комплексов лежат схожие принципы – блок тестируемого устройства обработки информации то переключается в активный (тестовый) режим работы, которому соответствуют специфичные и относительно просто выявляемые характеристики электромагнитного поля (ЭМП), то возвращается в пассивное состояние, при котором излучение минимально. Сопоставление особенностей радиоизлучения, наблюданного при пассивном и активном состоянии тестируемого блока, позволяет выявлять частоты информативных составляющих ПЭМИН. Вместе с тем конкретные методики обнаружения и изме-

рения составляющих ПЭМИН в комплексах различных производителей отличаются.

Рассмотрим возможности и методики работы с комплексами аппаратуры, базирующимися на комплексах радиомониторинга АРК-Д1ТИ [1, 2]. Можно выделить три возможных комплекта аппаратуры:

- ◆ **комплект 1.** Комплекс АРК-Д1ТИ с измерительными антеннами, пробником напряжения и вспомогательным генератором узкополосных сигналов;
- ◆ **комплект 2.** Комплекс АРК-Д1ТИ, снабженный управляемым с помощью беспроводной связи генератором сигналов АРК-ТГ3;
- ◆ **комплект 3.** Два комплекса АРК-Д1ТИ, связанные по беспроводному каналу, и генератор сигналов АРК-ТГ3, подключаемый непосредственно к управляющей ПЭВМ одного из комплексов.

Все комплекты содержат программное обеспечение (ПО), включающее:

- ◆ программу специальных измерений СМО-СИ РАПИРА (регистрация и анализ побочных излучений радиоэлектронной аппаратуры);
- ◆ программу управления режимами тестируемой аппаратуры СМО-ТЕСТЕР;

◆ программу расчета параметров защищенности технических средств обработки информации СМО-ПРИЗ.

Комплект 1 является базовым, он позволяет осуществлять все измерения и расчеты, предполагаемые действующими нормативно-методическими документами (НМД). Комплекты 2, 3 имеют расширенный состав. В комплекте 2 вспомогательный генератор используется при измерениях коэффициентов затухания сигналов и действующих высот случайных антенн. При этом беспроводная связь (БС) используется лишь для подачи команд на перестроение генератора. Как следствие, основным требованием является возможность перестройки генератора на любую частоту, а конкретный набор управляющих частот, используемых системой БС, принципиального значения не имеет. Вследствие этого при использовании комплекса АРК-Д1ТИ с дистанционно управляемым генератором АРК-ТГ3 для организации БС могут быть применены как аппаратура IEEE 802.11b/g (WiFi), так и различные узкополосные радиомодемы.

В комплекте 3 обмен данными между центральным и периферийным постами системы производится параллельно с проведением радиоизмерений, то есть используемые для БС частоты не должны принадлежать диапазону исследований. Среди средств коммуникации для ПЭВМ, удовлетворяющих подобным требованиям, предпочтительными с точки зрения дальности действия являются

устройства, работающие в соответствии со стандартами IEEE 802.11b/g (WiFi).

Задачи исследования защищенности информации от утечки по каналу ПЭМИН

Исследования ПЭМИН разделяются на задачи сертификации средств вычислительной техники (СВТ), используемых для обработки информации ограниченного доступа, и задачи аттестации объектов информатизации, на которых производится обработка подобных сведений. Целью сертификационных испытаний является решение задачи 1 – определение радиуса контролируемой зоны, внутри которой технически возможен перехват средствами разведки информативного сигнала, излучаемого исследуемым СВТ. Аттестация предполагает решение задачи 2 – исследования защищенности информации от утечки за счет ПЭМИН и задачи 3 – оценки эффективности принятых мер защиты информации от утечки по каналу ПЭМИН. Рассмотрим решение данных задач более подробно.

Задача 1 «Определение радиуса контролируемой зоны»

Сертификационные испытания, к которым относится задача 1, проводятся в лабораторных условиях при минимуме внешних воздействий и переотражений сигналов. Основные этапы решения задачи 1 перечислены в табл. 1.

Таблица 1. Основные этапы решения задачи расчета радиуса контролируемой зоны

Этап	Основной результат	Особенность использования полученных результатов
1. Выявление информативных составляющих ПЭМИН для разных блоков СВТ	список частот информативных составляющих ПЭМИН	полученный список частот определяет те составляющие ПЭМИН, интенсивность которых будет оцениваться на этапе 3; список передается для расчета в СМО-ПРИЗ (колонка, помеченная символом А на рис. 4)
2. Определение параметров тестовых сигналов	параметры тестовых сигналов	найденные параметры вносятся оператором в СМО-ПРИЗ
3. Определение опасных направлений и измерение интенсивностей составляющих ПЭМИН для блоков СВТ	измерение интенсивностей: <ul style="list-style-type: none">• смеси составляющих ПЭМИН и фонового шума;• интенсивности фонового шума в полосах составляющих ПЭМИН	найденные опасные направления в таблицы не заносятся, они используются при измерении интенсивностей составляющих ПЭМИН; результаты измерений передаются в СМО-ПРИЗ и отображаются на форме СМО-ПРИЗ в колонках В – Д (рис. 4)
4. Расчет радиуса контролируемой зоны	радиусы R_2 , r_1 и r_1' , характеризующие размеры контролируемой зоны*	отображаются в колонках, отмеченных на рис. 4 символом F, и автоматически вносятся в отчет по испытаниям

* R_2 – радиус зоны, внутри которой возможен перехват техническими средствами разведки информативного сигнала, излучаемого в эфир СВТ, с возможностью последующей обработки и расшифровки; r_1 – радиус зоны, внутри которой наводки на сосредоточенные случайные антенны имеют уровень, достаточный для регистрации техническими средствами разведки; r_1' – радиус зоны, внутри которой наводки на распределенные случайные антенны имеют уровень, достаточный для регистрации техническими средствами разведки.

Поскольку сертификационные испытания не предполагают измерения реальных коэффициентов затухания и/или показателей каких-либо случайных антенн, то все варианты аппаратной организации комплекса обеспечивают сопоставимые трудозатраты при выполнении измерений. Комплекс АРК-Д1ТИ с помощью программы СМО-ТЕСТЕР способен дистанционно переключать тестируемые блоки СВТ из пассивного состояния в активное и обратно. Это позволяет при выявлении информативных составляющих ПЭМИН использовать специальный режим, называемый режимом совмещенного обнаружения и тестирования информативности составляющих (ТОС) [3, 4]. Внедрение данного режима в программное обеспечение СМО-СИ РАПИРА в несколько раз сокращает временные затраты на поиск информативных составляющих ПЭМИН по сравнению с традиционным режимом раздельного обнаружения и тестирования информативных составляющих (ТОР).

Выполнение этапа 1 начинается с составления задания на исследование, в котором перечисляются все подлежащие тестированию блоки СВТ и частотные диапазоны, где будет выполняться поиск составляющих ПЭМИН. Затем оператор размещает антенну комплекса АРК-Д1ТИ вблизи подлежащего проверке блока СВТ (пока без тщательной подстройки ориентации и поляризации антенны), с помощью программы СМО-ТЕСТЕР подготавливает соответствующий блок к переключению в тестовый режим и подает команду на поиск сигналов (рис. 1). Через 5 – 15 мин (в зависимости от ширины тестового диапазона частот и особенностей настройки тестирования) оказывается сформированным предварительный список частот информативных составляющих ПЭМИН. Окончательный вариант списка частот определяется оператором после

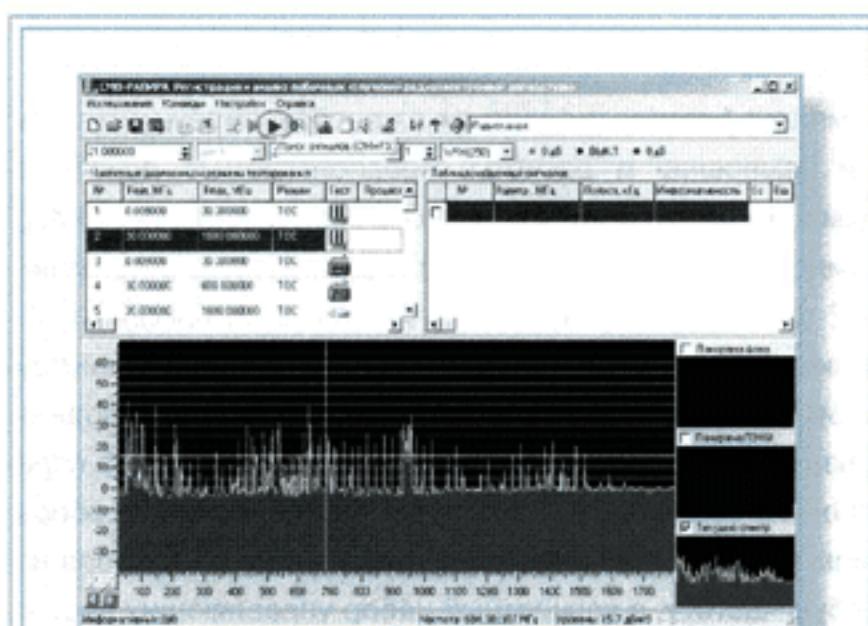


Рис. 1. Активация поиска информативных составляющих ПЭМИН монитора программой СМО-СИ РАПИРА 1.1

ручной перепроверки (необходимой при сложных условиях тестирования).

На этапе 2 параметры тестовых сигналов измеряются или рассчитываются оператором на основе сведений о функционировании тестируемого блока (ряд полезных рекомендаций можно также найти в [4]).

На этапе 3 СВТ размещают на поворотном столе, измерительную антенну устанавливают на расстоянии 1 м от СВТ (рис. 2) и переключают тестируемый блок в активный режим. Подбор направления для каждой составляющей осуществляется путем регулировки положения поворотного стола и направления поляризации измерительной антенны для обеспечения максимума интенсивности; измеряемое значение отображается на форме, показанной на рис. 3. Данный максимум фиксируется в таблице как результат измерения смеси составляющей ПЭМИН и фонового шума. Затем тестируемый блок физически выключается (возможно, вместе с проверяемым СВТ) и для всех частот составляющих автоматически измеряется напряженность поля фонового излучения в полосах составляющих ПЭМИН.

Собранные сведения сохраняются в файле данных программы СМО-СИ РАПИРА, затем по команде оператора передаются в программу СМО-ПРИЗ и



Рис. 2. Схема проведения измерения интенсивности информативных составляющих ПЭМИН при сертификационных испытаниях СВТ

используются для определения радиуса контролируемой зоны СВТ.

В соответствии с НМД для измерения напряженности поля используется пиковый или квазипиковый детектор с полосой пропускания, определяемой шириной спектра информативной составляющей ПЭМИН. Коэффициенты калибровки измерительной антенны учитываются автоматически.

На этапе 4 расчет радиуса контролируемой зоны начинается с передачи в программу СМО-ПРИЗ результатов измерений, накопленных программой СМО-СИ РАПИРА, а также с ввода оператором параметров тестовых сигналов. В программе СМО-ПРИЗ по расчетным формулам согласно НМД вычисляется напряженность поля нормированных шумов. Результаты расчетов по этим формулам для разных интервалов частот отображаются в СМО-ПРИЗ в колонках, отмеченных на рис. 4 символом Е. После получения всех необходимых данных для расчета программа СМО-ПРИЗ автоматически рассчитывает величины R_2 , r_1 , r_1' , характеризующие размеры контролируемой зоны, и оператору остается лишь распечатать отчет с результатами испытаний.

Поскольку целью сертификационных испытаний является оценка свойств лишь самого СВТ (без поправки на особенности конкретного помещения – объекта информатизации), то эти испытания не предполагают измерения реальных коэффициентов затухания и/или показателей каких-либо случайных антенн. Все измерения производятся вблизи исследуемой аппаратуры; вспомогательный генератор не требуется. В результате все варианты аппаратной организации комплекса обеспечивают сопоставимые трудозатраты.

Задача 2 «Исследование защищенности информации от утечки за счет ПЭМИН»

Решение задачи 2 производится в ходе аттестации объекта (либо рабочего места), на котором возможна обработка информации ограниченного доступа. Цель – проверить достаточность степени защищенности обрабатываемой информации от утечки по каналу ПЭМИН применительно к конкретному СВТ, размещенному в конкретной точке пространства. Подобные объектовые испытания позволяют учсть следующие условия использования СВТ.

- Геометрию границ контролируемой зоны объекта.

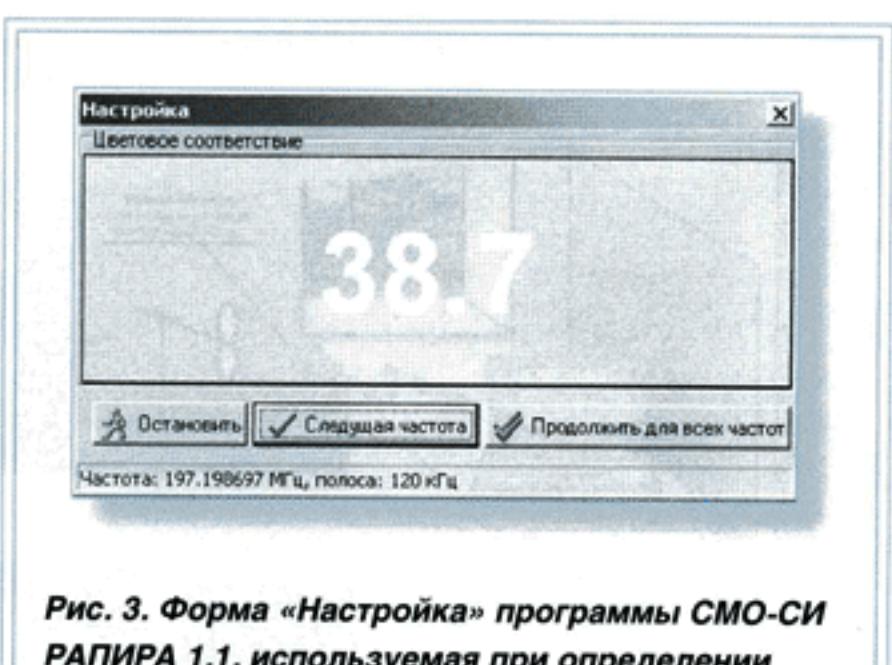


Рис. 3. Форма «Настройка» программы СМО-СИ РАПИРА 1.1, используемая при определении направления наиболее интенсивного излучения ПЭМИН

- Геометрию и особенности взаимного расположения помещений объекта.
- Реальные коэффициенты затухания (условия распространения) радиоволн.
- Наличие на объекте разнообразных случайных антенн и их характеристики.
- Возможности размещения аппаратуры радиоразведки вблизи объекта.

Уточним кратко возможные механизмы утечки информации, которые необходимо иметь в виду при проведении испытаний на объекте информатизации. СВТ, обрабатывая данные, порождает изменяющееся ЭМП, распространяющееся в окружающем его пространстве. По мере удаления от СВТ интенсивность составляющих ПЭМИН

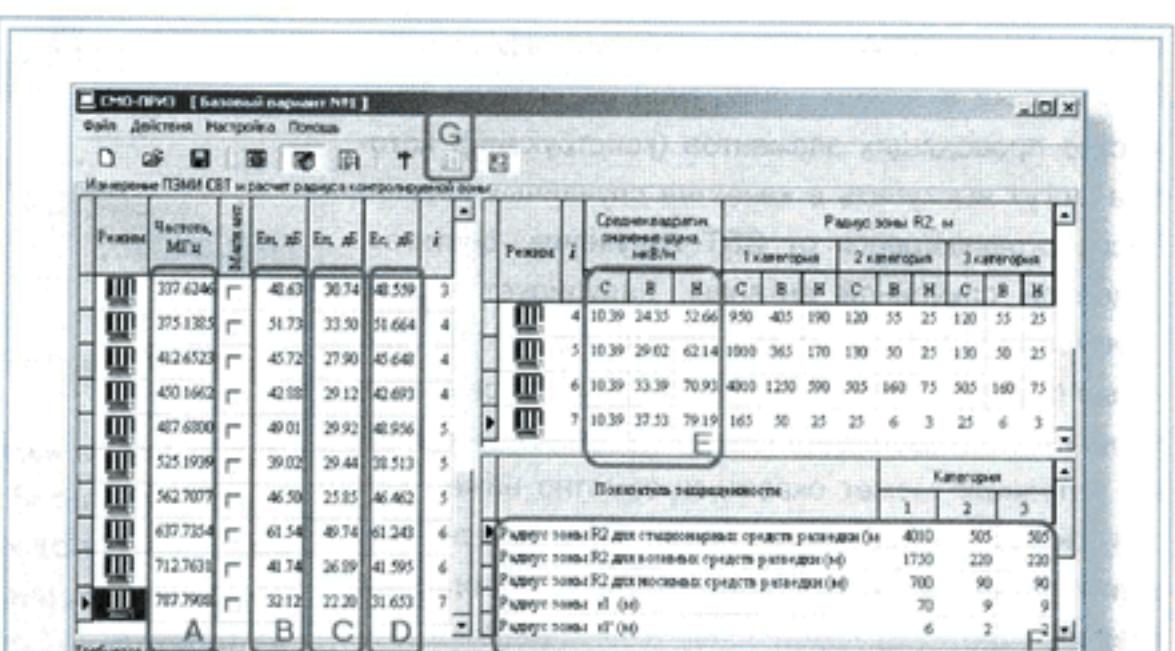
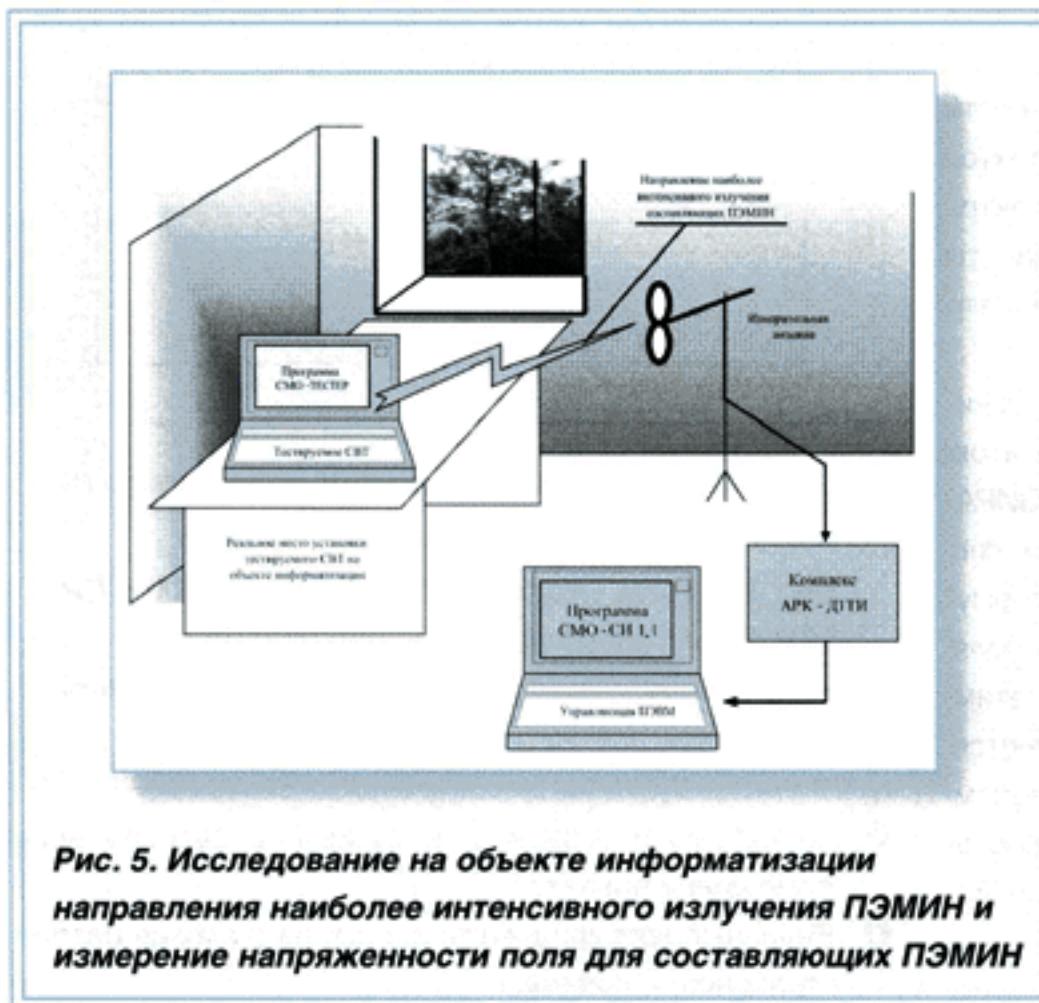


Рис. 4. Возможный вид главного окна программы СМО-ПРИЗ 1.1 при расчете радиуса контролируемой зоны



ослабевает, однако существует область пространства (ее размер приближенно определяется радиусом контролируемой зоны, полученным при решении задачи 1), в пределах которой отношение сигнал/шум остается достаточным для существования возможности восстановления информации, обрабатываемой СВТ. Таким образом, защищенность информации от утечки за счет ПЭМИН определяется степенью затухания информативных составляющих в местах возможного размещения средств разведки.

Возможен и другой механизм утечки информации. Практически в любом помещении существует множество проводящих элементов (конструкций), которые могут выступать в качестве случайных антенн. Распространяющееся от СВТ излучение, достигая подобной случайной антенны, индуцирует в ней переменное напряжение той же частоты. Далее принятый случайной антенной сигнал распространяется по ней как по длинной линии. При этом коэффициент затухания может оказаться заметно ниже, чем при «эфирном» распространении ЭМП, и если рассматриваемая проводящая конструкция выходит за пределы контролируемой зоны, то оказывается возможным снятие сигнала (контактное или бесконтактное) и его демодуляция (декодирование) средствами разведки, подключенными к данной линии утечки за пределами контролируемой зоны. Защищенность информации от утечки за счет наводок определяет-

ся затуханием составляющих ПЭМИН по ходу распространения до мест возможного размещения средств разведки.

Итак, контроль защищенности информации на объекте информатизации должен включать в себя как проверку возможности утечки информации за счет ПЭМИН, так и оценку опасности регистрации средствами разведки напряжений, наводимых в различных линиях. Основные этапы решения этой задачи перечислены в табл. 2. На реализации трех первых этапов мы не будем подробно останавливаться, поскольку методика их выполнения практически совпадает с задачей 1 с той лишь разницей, что исследования производятся непосредственно на объекте информатизации (рис. 5). Так как на первых трех этапах измерения производятся вблизи исследуемой аппаратуры без использования вспомогательного генератора, то состав комплекта аппаратуры не влияет на трудоемкость испытаний.

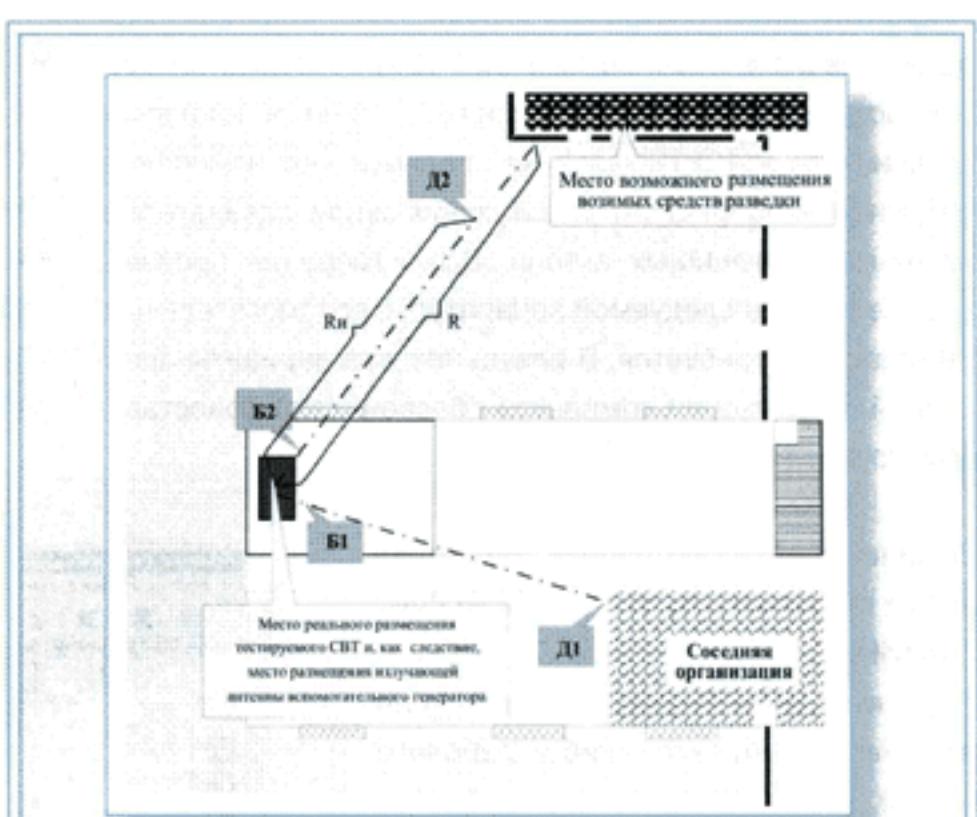


Рис. 6. Схема измерения коэффициентов затухания сигналов (этап 4) при оценке защищенности информации от утечки по каналу ПЭМИН на объекте информатизации. Б1, Д1 – места размещения измерительной антенны при измерениях коэффициентов затухания для носимых средств разведки, Б2, Д2 – места размещения измерительной антенны при измерениях коэффициентов затухания для возимых средств разведки

Таблица 2. Характеристики основных этапов решения задачи оценки защищенности информации от утечки за счет ПЭМИН

Этап	Основной результат	Особенность использования полученных результатов
1. Выявление информативных составляющих ПЭМИН для разных блоков СВТ	список частот информативных составляющих ПЭМИН	полученный список частот определяет те составляющие ПЭМИН, интенсивность которых будет оцениваться на этапе 3; список передается для расчета в СМО-ПРИЗ (колонка, помеченная символом А на (рис. 12)
2. Определение параметров тестовых сигналов	параметры тестовых сигналов	найденные параметры вносятся оператором в СМО-ПРИЗ
3. Определение опасных направлений и измерение интенсивностей составляющих ПЭМИН для блоков СВТ	измерение интенсивностей: • смеси составляющих ПЭМИН и фонового шума; • интенсивности фонового шума в полосах составляющих ПЭМИН	найденные опасные направления в таблицы не заносятся, они используются при измерении интенсивностей составляющих ПЭМИН; результаты измерений передаются в СМО-ПРИЗ и отображаются на форме СМО-ПРИЗ в колонках В – D (рис. 12)
4. Измерение реальных коэффициентов затухания сигналов в направлениях возможного размещения средств разведки	1) напряженности поля радиосигналов вблизи тестируемого СВТ на частотах информативных составляющих, формируемых вспомогательным генератором; 2) напряженности поля радиосигналов, регистрируемых при наблюдении тех же сигналов на границе контролируемой зоны или в иной достаточно удаленной точке	результаты измерений напряженности поля передаются в СМО-ПРИЗ, где по ним рассчитываются коэффициенты реального затухания сигналов; итоги измерений отображаются в СМО-ПРИЗ в колонках Е, F (рис. 12)
5. Измерение напряжений, наводимых в различных линиях утечки при работе блоков СВТ	наведенные напряжения: • смеси составляющих ПЭМИН и фонового шума; • фонового шума в полосах составляющих ПЭМИН	результаты измерений передаются в СМО-ПРИЗ, где по ним рассчитываются сигнальные составляющие наводок с поправкой на погрешности измерений; итоги измерений размещаются в колонках В – D (рис. 13)
6. Измерение коэффициентов затухания сигналов в исследуемой линии утечки	1) напряжения, индуцированные вспомогательным генератором в линии на частотах составляющих ПЭМИН; 2) напряжения, наблюдаемые в линии для тех же сигналов от вспомогательного генератора на границе контролируемой зоны	результаты измерений напряжений передаются в СМО-ПРИЗ, где по ним рассчитываются величины коэффициентов затухания; итоги измерений размещаются в СМО-ПРИЗ в колонке К (рис. 13)
7. Оценка действующей высоты случайной антенны для тестируемых линий утечки информации	1) напряжения, индуцируемые вспомогательным генератором в линии в точке, максимально близкой к тестируемому СВТ, на наборе контрольных частот; 2) напряженность поля, наблюдаемая для тех же сигналов вспомогательного генератора вблизи тестируемой линии	результаты измерений напряжений и напряженности поля передаются в СМО-ПРИЗ, где по ним рассчитывается действующая высота антенны на контрольных частотах
8. Расчет показателей защищенности информации	отношения сигнал/шум, наблюдаемые на границе контролируемой зоны	отображаются в колонках, отмеченной на рис. 12, 13 символами G, H, и автоматически вносятся в отчет испытаний

Целью выполнения этапа 4 является оценка коэффициентов затухания высокочастотных сигналов, реально наблюдаемых на объекте информатизации и определяющих для сигналов ПЭМИН отношение сигнал/шум, наблюдаемое на границе контролируемой зоны. Измерение коэффициентов затухания предусматривает излучение вспомогательным генератором тестовых сигналов на час-

тах информативных составляющих ПЭМИН с замером интенсивности поля вблизи и на существенном удалении от генератора. Для обеспечения точности измерений кабель, подсоединяющий измерительную antennу к входу измерительного приемника, должен иметь небольшую длину. Как следствие, производить измерения одновременно в ближней и дальней точке при наличии одного

измерительного комплекса невозможно; эти измерения приходится делать последовательно друг за другом.

Рассмотрим последовательность действий, которую должен выполнить оператор, использующий комплект аппаратуры 1 (базовый комплект).

- 1 Тестируемое СВТ выключается, в месте его размещения устанавливается излучающая антenna вспомогательного генератора сигналов (перечень рекомендемых генераторов можно найти в НМД).
- 2 Комплекс АРК-Д1ТИ размещается вблизи от места установки тестируемого СВТ, а его измерительная антenna устанавливается на расстоянии 1 м от антенны вспомогательного генератора. Так, при измерении коэффициентов затухания сигналов применительно к носимым средствам разведки для размещения измерительной антены можно рекомендовать точку Б1, показанную на рис. 6. При проведении измерений по отношению к возимым средствам разведки для размещения измерительной антены можно рекомендовать точку Б2.
- 3 Оператор выбирает в выпадающем списке формы СМО-СИ РАПИРА в качестве тестируемой линии утечки «Радиоканал» и подает команду «Измерение уровней сигналов вблизи от РЭА» для первого частотного диапазона из задания на тестирование.
- 4 Начало выполнения измерения влечет появление на экране ПЭВМ формы «Настройка», которая в данном случае имеет вид, показанный на рис. 7. Частота в верхней части формы соответствует первой из информативных составляющих ПЭМИН текущего диапазона. Оператор перестраивает вспомогательный генератор на указанную частоту и затем подбирает положение измерительной антены, обеспечивающее максимальное значение результата измерений.
- 5 После нажатия на форме кнопки «Следующая частота» программа СМО-СИ записывает в своей базе данных результат текущего измерения, перестраивает приемный тракт комплекса АРК-Д1ТИ на измерение напряженности поля на частоте следующей информативной составляющей ПЭМИН текущего частотного диапазона и предлагает оператору настроить на эту частоту вспомогательный генератор. Поскольку излучающая и измерительная антены к этому моменту уже сориентированы относительно друг друга, то подстройки положения антенн больше не требуется.
- 6 В результате подобного «пошагового» процесса фиксируются значения напряженности поля

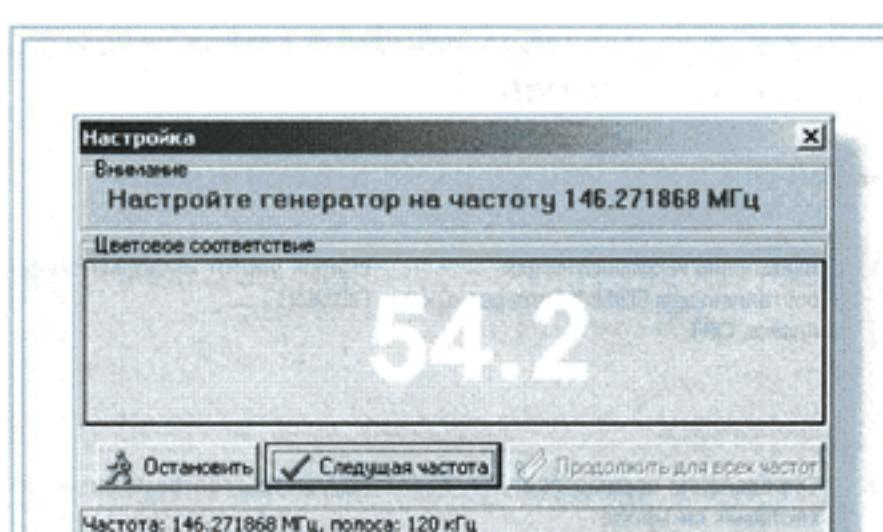


Рис. 7. Форма «Настройка» при оценке коэффициентов затухания

для всех частот данного частотного диапазона. Затем аналогичные измерения проводятся для всех других поддиапазонов; при этом помимо перестройки по частотам вспомогательного генератора от оператора требуется лишь следить за правильностью выбора используемой измерительной антены.

- 7 После завершения измерений вблизи СВТ измерительный комплекс перемещают на границу контролируемой зоны. Применительно к ситуации, представленной на рис. 6, при оценке коэффициентов затухания сигналов для носимых средств разведки можно порекомендовать разместить измерительную антенну в точке Д1. Если же размещение измерительной

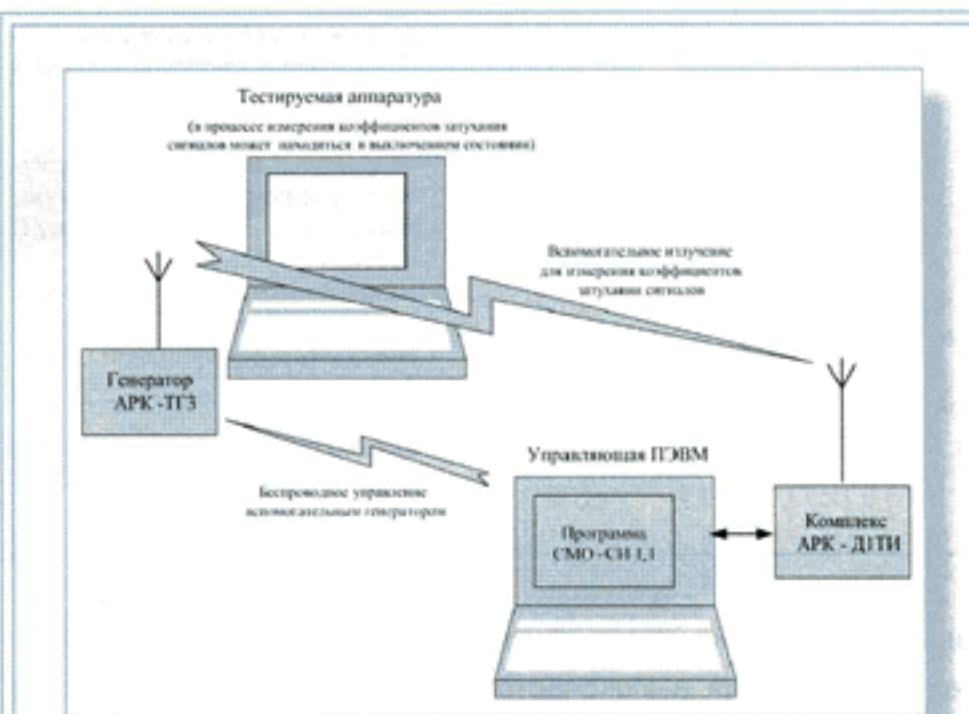


Рис. 8. Измерение интенсивности вспомогательных сигналов в удаленной точке комплексом аппаратуры с управляемым генератором

антенны непосредственно на границе контролируемой зоны затруднительно, то для получения данных можно выбрать некоторую промежуточную точку (подобную точке Д2 для возимых средств разведки на рис. 6) с фиксацией расстояния, на котором реально проводились измерения.

- 3 Оператор измеряет напряженности поля в удаленной от СВТ точке командой программы СМО-СИ «Измерение уровней сигналов вдали от РЭА» и повторно выполняет описанные выше действия. Следует отметить, что проводить при этом измерения удобнее вдвоем, так как рекомендуемые НМД генераторы дистанционного управления не предусматривают, а значит, помимо самого оператора, контролирующего процесс измерений, необходим помощник, обеспечивающий перестроение вспомогательного генератора.

Таким образом, при определении коэффициентов затухания неудобство комплекта 1 состоит в том, что вспомогательный генератор и измерительный приемник разнесены в пространстве и выполняяший измерения оператор вынужден тратить значительное время на перемещение между точками размещения вспомогательного генератора и измерительной аппаратуры или использовать помощника. Заметный дополнительный расход времени вызывается при этом и самой процедурой «ручной» перестройки генератора на нужные частоты.

Если вместо комплекта 1 воспользоваться комплектом 2 с управляемым генератором, то ситуация упрощается.

Для проведения измерений вдали от СВТ генератор АРК-ТГЗ с излучающей антенной размещают вблизи тестируемого устройства обработки информации, а оператор с измерительным комплексом АРК-Д1ТИ располагается в точке проведения удаленных измерений (рис. 8). Благодаря дистанционному беспроводному управлению генератором исключается необходимость «ручной» настройки генератора, что существенно ускоряет переход с частоты на частоту, кроме того, оператор может управлять процедурой перестройки из удаленной точки.

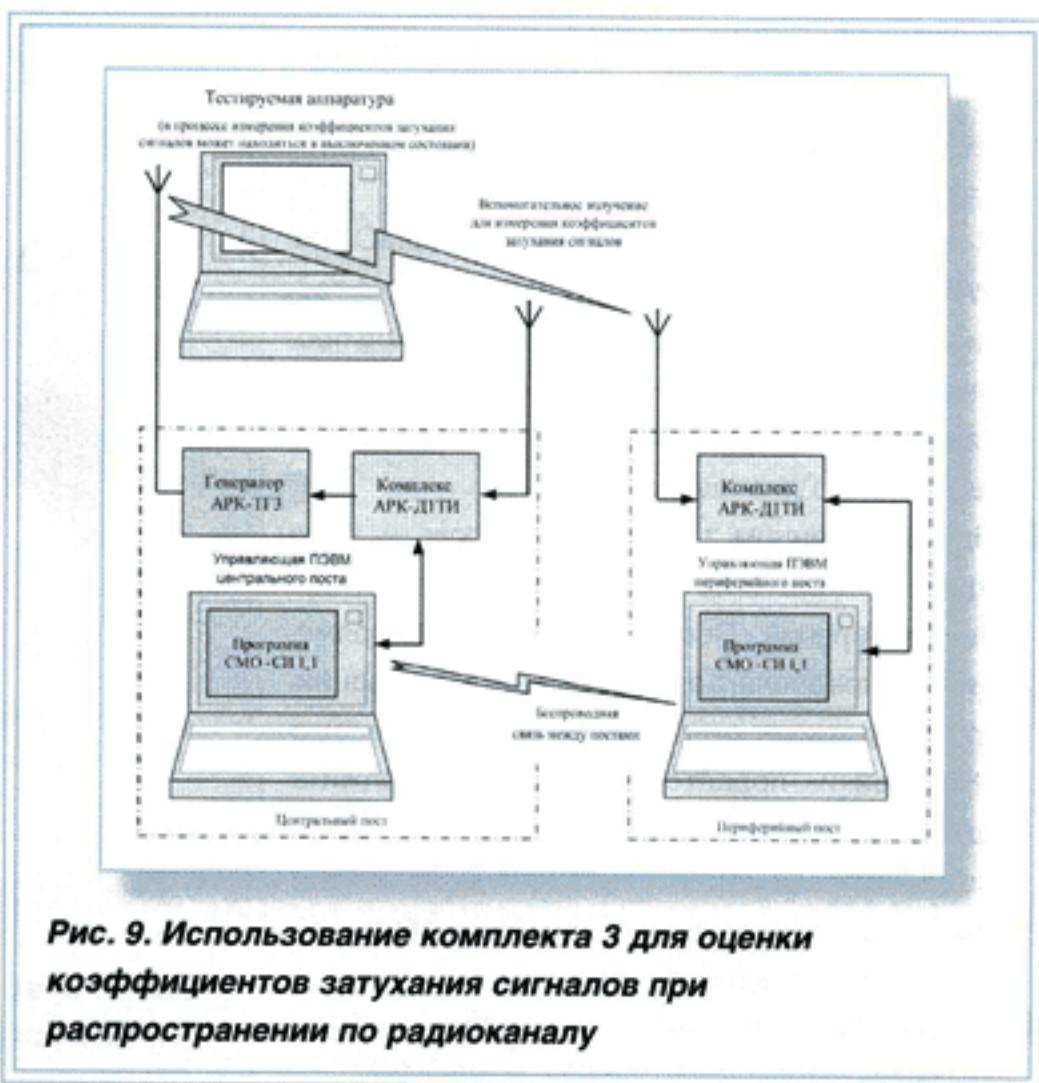
Еще больший выигрыш достигается при использовании комплекта 3. При ситуации, рассмотренной на рис. 6, центральный пост устанавливают в точках Б1 и Б2, а периферийный – в точках Д1 и Д2 и вместо раздельного измерения интенсивностей сигналов вблизи и вдали от СВТ производят те же измерения двумя комплексами параллельно, используя команду СМО-СИ РАПИРА «Измерение уровней сигналов вблизи/вдали от РЭА».

Проведение измерений в ближней и дальней точке параллельно во времени (рис. 9) не только заметно ускоряет получение данных, но и гарантирует более высокую точность определения коэффициентов затухания. Дело в том, что при измерениях с разрывом во времени, что неизбежно при использовании комплектов 1 или 2 за прошедший с начала измерений интервал времени, радиооборудование в исследуемых диапазонах частот может существенно измениться, что может стать причиной ошибок.

Этапы 5 – 6 оценивания защищенности информации от утечки по каналу ПЭМИН предполагают детальное исследование свойств имеющихся на объекте каналов утечки информации. Основой для подобных каналов могут, к примеру, выступать следующие линии:

- ◆ осветительная и силовая сети или незадействованные в данный момент провода (с обрывом);
- ◆ телефонная линия и линия пожарной сигнализации;
- ◆ инженерные коммуникации (система вентиляции, отопления и др.);
- ◆ металлические конструкции (например, карниз), идущие в помещениях и расположенные вблизи мест размещения СВТ.

До начала выполнения этапов 5 – 6 линии, подлежащие тестированию, вносятся в программу СМО-СИ РАПИРА в виде списка на форме «Параметры программы». В процессе сбора данных все внесенные в этот список линии оказываются доступными в выпадающем списке



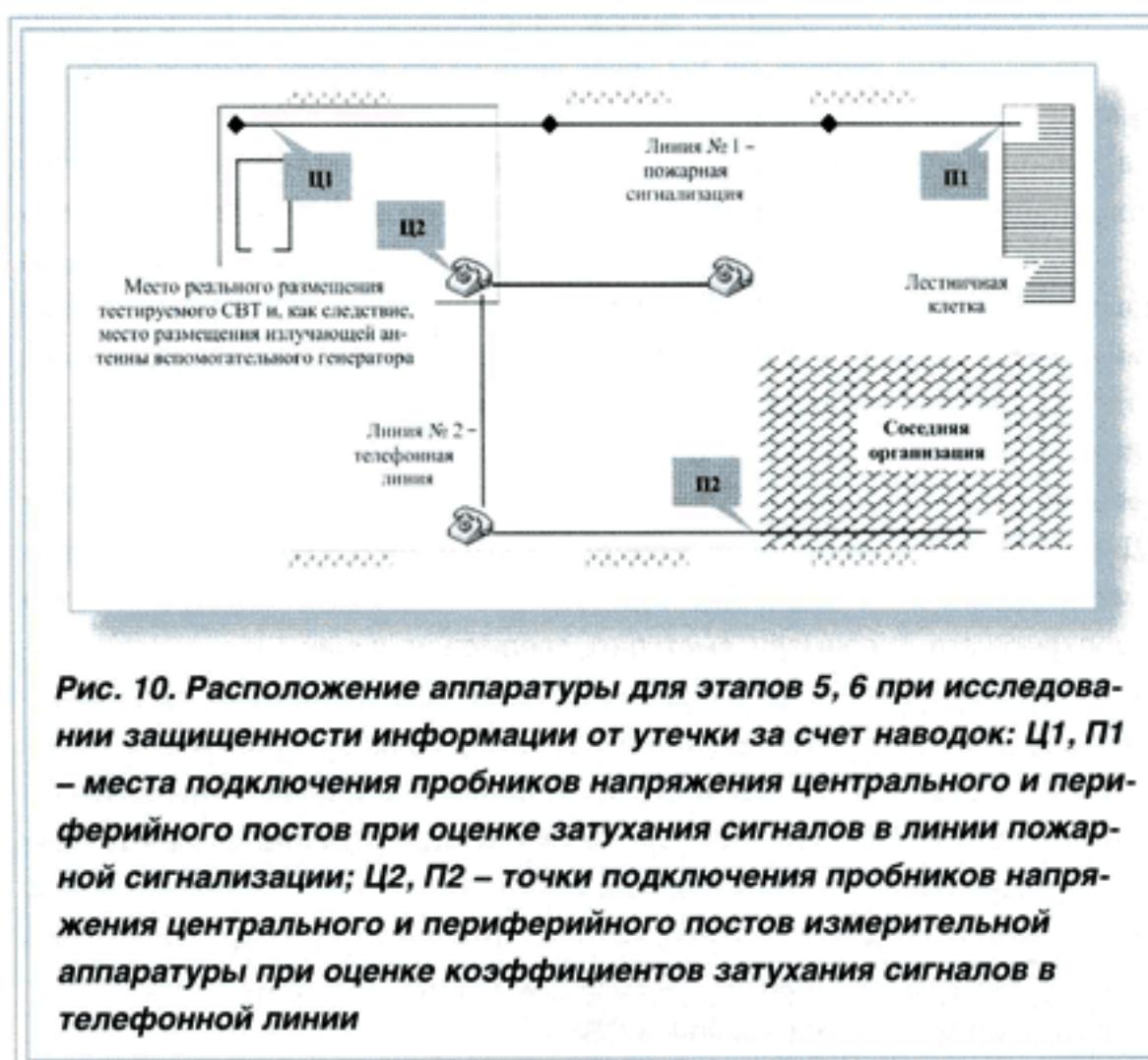


Рис. 10. Расположение аппаратуры для этапов 5, 6 при исследовании защищенности информации от утечки за счет наводок: Ц1, П1 – места подключения пробников напряжения центрального и периферийного постов при оценке затухания сигналов в линии пожарной сигнализации; Ц2, П2 – точки подключения пробников напряжения центрального и периферийного постов измерительной аппаратуры при оценке коэффициентов затухания сигналов в телефонной линии

на панели управления СМО-СИ РАПИРА. Данный список включает «Радиоканал», выбор которого предполагает исследование ПЭМИН и, значит, использование при сборе данных измерительных антенн. Все остальные каналы утечки считаются линиями наводок и, следовательно, при проведении измерений предполагают использование пробника напряжения.

Измерение интенсивности наведенных напряжений производится в следующем порядке.

- ❶ В выпадающем списке в программе СМО-СИ РАПИРА оператор выбирает подлежащую тестированию линию и подключает к ней вход пробника напряжения. Выход пробника соединяется с антенным входом аппаратуры АРК-Д1ТИ для данного диапазона частот.
- ❷ При включенном тестируемом блоке и запущенном teste оператор активирует выполнение измерений. Поскольку пробник напряжения не предполагает настройки поляризации, то сразу после старта измерений на форме «Настройки» подается команда «Продолжить для всех частот», что позволит максимально быстро замерить интенсивности смеси наведенных напряжений ПЭМИН с наводками иного происхождения.
- ❸ После фиксации значений напряжений по подсказке программы СМО-СИ РАПИРА опе-

ратор выключает тестируемый блок и повторяет измерения на всех частотах текущего поддиапазона для регистрации напряжений, имеющих отличающуюся от ПЭМИН природу.

- ❹ Аналогичные действия повторяются для всех прочих частотных диапазонов, содержащих информативные составляющие ПЭМИН и для всех имеющихся линий.
- ❺ Собранные сведения сохраняются в файле данных программы СМО-СИ РАПИРА и по команде оператора передаются в программу СМО-ПРИЗ для определения напряжения сигнальных составляющих компонент ПЭМИН для каждого из каналов утечки.

Целью выполнения этапа 6 является оценка коэффициентов затухания высокочастотных сигналов при их распространении по тестируемой линии.

Как и для радиоканала, измерение

коэффициентов затухания предусматривает формирование вспомогательным генератором тестовых сигналов на частотах информативных составляющих ПЭМИН с замером интенсивности сигналов вблизи и на существенном удалении от генератора, однако измерению теперь под-

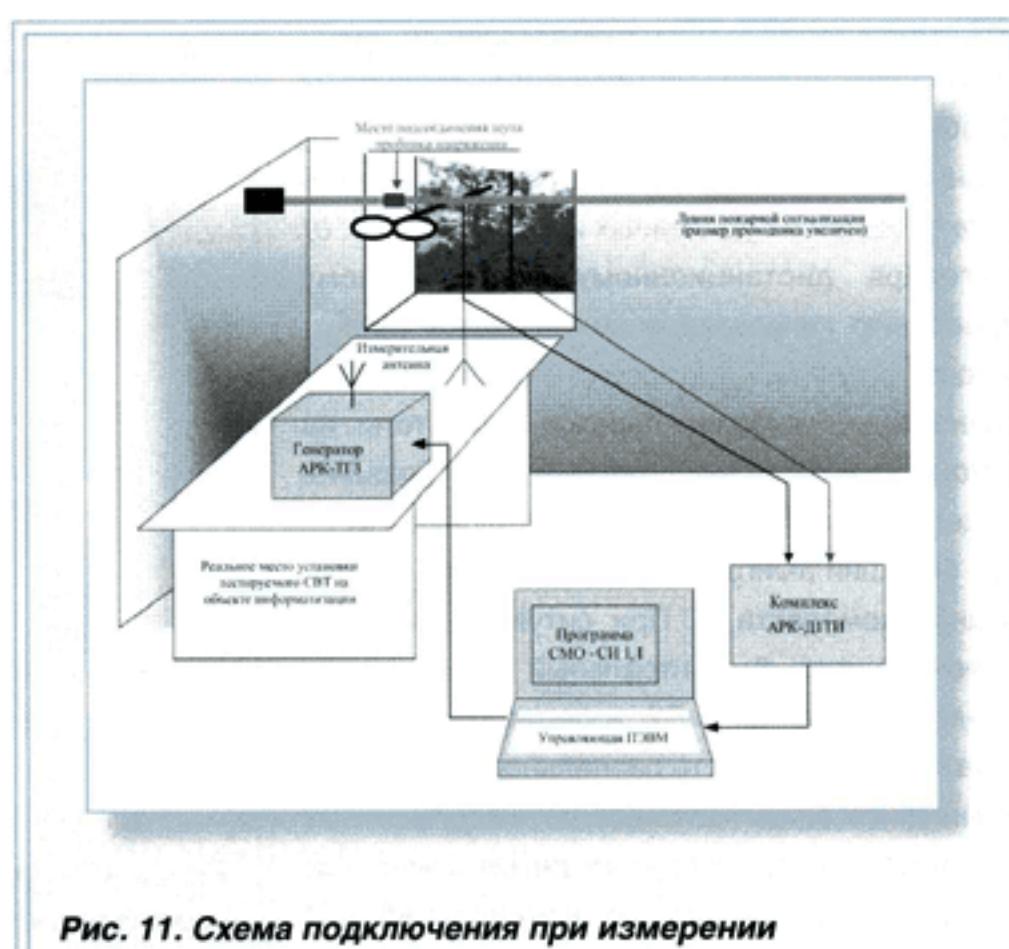


Рис. 11. Схема подключения при измерении действующих высот случайных антенн

лежат наведенные напряжения, наблюдаемые в исследуемой линии. При использовании комплекта аппаратуры З последовательность действий такова.

- 1 С помощью генератора сигналов АРК-ТГЗ, входящего в состав центрального поста системы, в проверяемой линии индуцируется напряжение сигнала.
- 2 Центральный пост размещается вблизи от места установки тестируемого СВТ, а подключенный к нему пробник напряжения присоединяется к ближайшей к СВТ точке проверяемой линии. Периферийный пост размещается вблизи границы контролируемой зоны и его пробник также присоединяется к проверяемой линии. Пример возможного размещения постов системы показан на рис. 10.
- 3 Оператор выбирает в выпадающем списке тестируемую линию и активирует процедуру измерений командой «Измерение уровней сигналов вблизи/вдали от РЭА».
- 4 Сразу после появления на экране ПЭВМ формы «Настройка» оператор подает команду «Продолжить для всех частот». По этой команде управляющая ПЭВМ центрального поста начинает перестраивать генератор АРК-ТГЗ с частоты на частоту, выполняя одновременные измерения двумя комплексами на каждой из частот.
- 5 Аналогичные измерения проводятся для всех частотных поддиапазонов задания всех подлежащих проверке линий. В процессе перебора частот и линий задачей оператора является физическое переключение щупа пробника с одной тестируемой линии на другую.
- 6 Собранные сведения сохраняются в файле данных программы СМО-СИ РАПИРА, далее по команде

оператора передаются в программу СМО-ПРИЗ для определения коэффициентов затухания сигналов.

Как и при измерении коэффициентов затухания сигналов в радиоканале, использование вместо комплекта З комплекта 2 приводит к снижению скорости сбора данных. Применение комплекта 1 сопряжено со значительными потерями времени на «ручную» перестройку с частоты на частоту вспомогательного генератора.

Оценка действующих высот случайных антенн, выполняемая на этапе 7, необходима для последующего пересчета программой СМО-ПРИЗ напряженности поля нормированных шумов в шумовую составляющую наведенного напряжения, на фоне которой осуществляется перехват информации средствами разведки. Зависимость действующей высоты антенны от частоты обычно оказывается относительно плавной, поэтому измерения на данном этапе проводят на небольшой по объему сетке фиксированных частот. Основные действия, проводимые на этом этапе, сводятся к следующему.

- 1 Тестируемое СВТ выключается, и на месте его размещения устанавливается излучающая антenna вспомогательного генератора сигналов. Измерительная антenna размещается на расстоянии не более 0,5 м от тестируемой линии так, чтобы при наведении в ней напряжения вспомогательным генератором на выходе измерительной антены наблюдался сигнал максимальной интенсивности (рис. 11). К самой линии рядом с измерительной антенной подключается щуп пробника напряжения.
- 2 Оператор запускает процедуру измерений командой «Измерение напряженности ЭМП и наводок». При этом вспомогательный генератор либо автоматичес-

Регион	Частота, МГц	Изл. dB	Изл. dB	Изл. dB	Изл. dB	Возможные		Несущие				
						Крз, dB	Выч. нейтр.	Осл. реф.	Крз, dB	Выч. нейтр.	Осл. реф.	
	375.0285	Г	31.73	33.30	31.654	-4	40.13	24.3	0.096	41.60	32.7	0.096
	402.6520	Г	45.72	27.98	41.64	-4	40.04	24.3	0.096	40.52	32.7	0.096
	406.0662	Г	42.88	29.12	42.670	-4	40.44	24.3	0.096	40.90	32.7	0.096
	487.0230	Г	49.0	29.30	42.95	-3	40.80	29.0	0.096	40.28	42.1	0.096
	521.1939	Г	19.62	29.40	30.313	-3	40.13	29.0	0.096	41.58	42.1	0.096
	562.7077	Г	46.20	25.12	46.462	-3	44.33	29.0	0.096	40.10	42.1	0.096
	607.7354	Г	63.54	49.74	61.240	-4	40.53	30.4	0.291	40.30	73.9	0.201
	712.7610	Г	48.74	26.89	40.595	-4	40.60	33.4	0.291	39.38	73.9	0.201
							G	F			H	
	A	B	C	D	E							

Рис. 12. Возможный вид главного окна программы СМО-ПРИЗ 1.1 при расчете защищенности информации на объекте информатизации по каналу ПЭМИН

Регион	Частота, МГц	Изл. dB	Изл. dB	Изл. dB	Изл. dB	Возможные		Несущие				
						Крз, dB	Выч. нейтр.	Осл. реф.	Крз, dB	Выч. нейтр.	Осл. реф.	
	375.0285	Г	56.20			56.700	1	40.52	1170.4	0.028	1136.4	0.028
	712.7377	Г	55.30			55.300	1	38.36	1170.4	0.028	1136.4	0.028
	112.5462	Г	51.20			51.200	1	35.92	1170.4	0.028	1136.4	0.028
	130.0354	Г	67.10			68.800	2	53.34	40.7	0.712	39.6	0.712
	187.5662	Г	74.70			74.700	2	47.96	40.7	0.912	39.6	0.912
	220.0021	Г	74.40			74.400	2	47.96	40.7	0.912	39.6	0.912
	363.7946	Г	65.20			68.300	3	48.15	37.8	0.260	32.9	0.130
	366.1168	Г	53.90			55.900	3	40.02	37.8	0.260	32.9	0.130
	A	B	C	D	E				K		G	H

Рис. 13. Вид главного окна программы СМО-ПРИЗ 1.1 при расчете защищенности информации на объекте информатизации применительно к линиям наводок

Таблица 3. Заключительные этапы решения задачи 3 оценки эффективности принятых мер защиты информации

Этап	Основной результат	Особенность использования полученных результатов
7. Измерение интенсивности шума, формируемого системой САЗ в разных линиях утечки	напряженность поля или наведенное шумовое напряжение для задаваемой оператором сетки контрольных частот	результаты измерений передаются в СМО-ПРИЗ, где по ним определяют напряженность помех, на фоне которых действуют составляющие ПЭМИН
8. Измерение коэффициентов затухания шума САЗ в разных линиях	выполняется аналогично п. 4, 6 задачи 2	результаты измерения интенсивности сигналов вспомогательного генератора вблизи и вдали от генератора шума передаются в СМО-ПРИЗ, где с учетом удаленности средств разведки производится расчет коэффициентов затухания шума
9. Расчет показателей защищенности информации	отношения сигнал/шум, наблюдаемые на границе контролируемой зоны	отображаются в колонках таблицы, отмеченных на рис. 14 символами G – H, и автоматически вносятся в отчет испытаний

ки настраивается на нужную частоту из имеющегося списка контрольных частот (при использовании комплектов 2 или 3), либо на экран выводится приглашение оператору осуществить необходимую настройку генератора вручную. При подтверждении оператором готовности программа СМО-СИ РАПИРА замеряет наведенное в линии напряжение и напряженность поля, порождаемые вспомогательным генератором, и переходит к измерениям на следующей частоте.

- 3 После выполнения измерений по списку частот для данной линии оператор повторяет измерения для других линий.

Так как все измерения производятся вблизи тестируемого СВТ и, следовательно, могут быть осуществлены одним измерительным комплексом, то комплектность аппаратуры значимого влияния на эффективность выполнения данного этапа не оказывает.

На этапе 8 производится расчет совокупности отношений сигнал/шум на границе контролируемой зоны. После передачи результатов измерений в расчетную программу СМО-ПРИЗ выполняются следующие действия.

- 1 Оператор вводит параметры тестовых сигналов в форму «Параметры режимов тестирования СВТ», а сведения о возможном размещении средств разведки и о параметрах проведения измерений – в форму «Параметры программы».
- 2 При запрете автоматического пересчета коэффициентов затухания оператор обязан вручную ввести или с использованием расчетных форм определить коэффициенты реального затухания радиосигналов и затухания наведенных напряжений в линиях утечки, а также действующие высоты тестируемых случайных

антенн; если же флаг «Автоматический пересчет коэффициентов затухания» установлен, то программа СМО-ПРИЗ сама заполнит колонки таблиц значениями и коэффициентами, соответствующими переданным результатам измерений.

- 3 Активируется процедура расчета показателей защищенности, результаты которой представлены на рис. 12, 13 в колонках, отмеченных символами G – H; при установленном флаге «Автоматический пересчет показателей» для получения показателей защищенности действий оператора не требуется.

На этом расчет показателей защищенности завершается, и оператору остается лишь распечатать отчет с результатами испытаний.

Задача 3 «Оценка эффективности принятых мер защиты информации от утечки по каналу ПЭМИН»

На объектах информатизации, оборудованных системой активной защиты (САЗ), перехвату информации помимо естественных шумов препятствует активная помеха, формируемая генератором шума. С учетом этого при расчете показателей защищенности информации необходимо учитывать:

- ◆ интенсивность шума, формируемого системой САЗ;
- ◆ коэффициент качества генерируемого шума;
- ◆ взаимное расположение антennы генератора шума и защищаемой ПЭВМ.

Нормальное функционирование системы САЗ предполагает, что интенсивность создаваемых ею помех в точках возможного размещения средств разведки существенно превосходит уровень естественных шумов, поэтому при анализе защищенности информации принимается во внимание лишь шум, создаваемый системой САЗ, а

последовательность испытаний дополняется этапом измерения характеристик этого шума.

Первые 6 этапов аттестации объектов, оборудованных системой САЗ, не отличаются от аналогичных этапов решения задачи 2, поэтому рассмотрим лишь заключительные этапы решения задачи 3, которые приведены в табл. 3.

При проведении аттестационных испытаний измерения интенсивности ПЭМИН и параметров САЗ приходится производить на фоне многочисленных внешних электромагнитных помех. Это означает, что при измерении интенсивности шума, формируемого генератором шума САЗ, измеряется интенсивность смеси этого шума с «посторонними» излучениями. Как следствие, результаты измерений интенсивности шума на частотах, занятых мощными радиовещательными станциями, почти наверняка будут иметь существенную погрешность.

При выполнении этапа 7 данная особенность учитывается следующим образом. Вместо выполнения замеров шума на всех смежных участках оси частот в программе СМО-СИ РАПИРА предусмотрено использование разреженной сетки частот, параметры которой до измерений задаются оператором. В окрестности каждой точки выбранной сетки частот программа выполняет несколько независимых измерений на разных частотных интервалах шириной около 1 МГц и отыскивает участок, где усредненная интенсивность наблюдаемого сигнала оказывается наименьшей. Такой подход позволяет с высокой вероятностью минимизировать влияние внешней радиообстановки на результаты измерений, а интенсивность шума САЗ на частотах, где измерений не производилось, будет аппроксимирована программой СМО-ПРИЗ (в предположении, что на интервале в несколько МГц существенных изменений в интенсивности излучения генератора шума быть не должно). В качестве дополнительной меры защиты результатов измерений от влияния внешних помех программа СМО-СИ РАПИРА позволяет оператору визуально исследовать спектр радиоизлучений в окрестности любой из точек измерения и убедиться, что существенных по уровню помех в области измерений нет, в противном случае исключить неудачную точку из процедуры измерения.

Поскольку генератор системы САЗ не требует какого-либо управления со стороны измерительной аппаратуры, а выполнение этапа 7 не предполагает измерений в удаленных точках, то использование комплекта 2 не дает никаких преимуществ по отношению к базовому комплекту 1. В системе из двух взаимодействующих комплексов можно было бы добиться некоторого ускорения

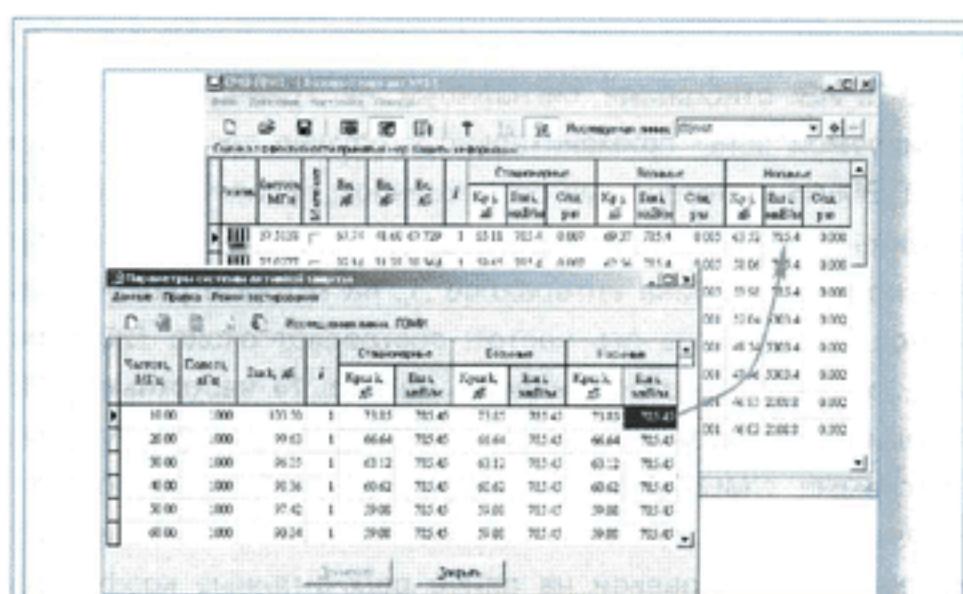


Рис. 14. Возможный вид окна «Параметры системы активной защиты» программы СМО-ПРИЗ 1.1 при оценке эффективности средств защиты информации на объекте информатизации

измерений за счет проведения параллельных измерений для разных линий, однако текущий релиз программного обеспечения СМО-СИ РАПИРА таких возможностей пока не предоставляет. Таким образом, комплектность аппаратуры на эффективность выполнения этапа 7 влияния не оказывает.

Выполнение этапа 8 отличается от этапов 4, 6 (из задачи 2) лишь тем, что измерение коэффициентов затухания производится не в точках размещения составляющих ПЭМИН, а на частотах измерения интенсивности шума САЗ.

Завершающий этап расчета показателей защищенности информации осуществляется программой СМО-ПРИЗ и подразумевает следующие действия.

- ➊ Получение результатов измерения интенсивности составляющих ПЭМИН и параметров системы САЗ из программы СМО-СИ РАПИРА.
- ➋ Уточнение параметров тестовых сигналов и сведений о размещении антенны генератора шума системы САЗ и о местах возможного размещения средств разведки противника. Эти данные оператор настраивает на формах «Параметры программы» и «Параметры режимов тестирования СВТ».
- ➌ Перерасчет коэффициентов затухания для сигналов ПЭМИН и излучения системы САЗ, активизируемый оператором или стартующий автоматически (в случае установки флага «Автоматический перерасчет коэффициентов затухания»).
- ➍ Расчет среднеквадратической интенсивности шума САЗ применительно к каждому из режимов тестирования и отношений сигнал/шум, наблюдавшихся на границе контролируемой зоны.

На рис. 14 представлен пример расчета программой СМО-ПРИЗ отношения сигнала/шум на границе контролируемой зоны применительно к случаю тестирования ПЭМИН монитора при совмещенном расположении антенны генератора шума и защищаемого СВТ. В данном примере ширина интервалов Δ_i , на которые разбивается при анализе ось частот, составляет около 120 МГц, поэтому все отображаемые на рис. 14 частотные позиции относятся к первому частотному интервалу. Программа СМО-ПРИЗ, аппроксимируя сведения об излучении генератора шума на интервал между точками измерений с поправкой на ранее рассчитанные коэффициенты затухания, рассчитывает для интервала Δ_i среднеквадратическую напряженность шума, пересчитанную к границе контролируемой зоны. Напряженность шумового поля во всех строках формы «Параметры системы активной защиты», отображаемой на рис. 14, одна и та же из-за того, что все эти строки относятся к одному и тому же частотному интервалу. Рассчитывая отдельно суммарную мощность составляющих ПЭМИН, принадлежащих тому же интервалу Δ_i , учитывая соответствующие им коэффициенты затухания и сравнивая найденную таким образом интенсивность сигнала с уже полученной среднеквадратической напряженностью шума, программа СМО-ПРИЗ оценивает отношение сигнал/шум на границе контролируемой зоны с учетом работы системы САЗ. Это значение отображается на главной форме программы (колонки с заголовком «С/ш, раз») и характеризует защищенность информации на объекте информатизации.

После расчета отношений сигнал/шум для всех частотных интервалов и всех линий утечки анализ защищенности информации оказывается завершенным, и оператору остается лишь распечатать отчет с результатами испытаний.

Заключение

В статье проанализирована современная методика исследования защищенности информации от утечки по каналу ПЭМИН, разъяснена суть основных этапов исследования, проиллюстрированы отдельные операции, традиционно вызывающие затруднения при проведении специальных исследований. Показано, что все рассмотренные задачи ПЭМИН решаются с помощью комплектов измерительной аппаратуры на базе комплекса радиомониторинга АРК-Д1ТИ.

Применение аппаратуры АРК-Д1ТИ и специального программного обеспечения СМО-СИ РАПИРА и СМО-ПРИЗ для решения задач оценки защищенности информации от утечки по каналу ПЭМИН автоматизирует большинство измерительных и расчетных операций. При этом для проведения сертификации средств СВТ эффективным оказывается базовый комплект измерительной аппаратуры, включающий лишь комплекс АРК-Д1ТИ с измерительными антеннами, а при аттестации объектов информатизации использование базового комплекта сопряжено с большими затратами времени, например при измерении коэффициентов затухания сигналов. Для снижения трудоемкости измерений в ходе аттестационных испытаний рекомендуется применение расширенных комплектов аппаратуры.

Комплекс АРК-Д1ТИ, снабженный управляемым с помощью беспроводной связи генератором сигналов АРК-ТГЗ, существенно ускоряет проведение исследований за счет того, что оператор управляет генератором дистанционно, перестройка генератора происходит автоматически. Комплект аппаратуры из двух связанных беспроводной сетью комплексов АРК-Д1ТИ обеспечивает повышение точности и сокращение времени определения коэффициентов затухания за счет параллельных измерений в ближней и дальней точках.

Литература

1. АРК-Д1ТИ – многофункциональный портативный комплекс радиомониторинга. Сертификат Госстандарта РФ об утверждении типа средств измерений RU.C.35.002.А № 13618 от 03.12.02, зарегистрирован в Государственном реестре средств измерений под № 23924-02.
2. АРК-Д1ТИ – многофункциональный портативный комплекс радиомониторинга и выявления технических каналов утечки информации. Сертификат ФСТЭК № 506/1 от 01.02.05.
3. Тупота В.И., Бегишев М.Р., Козьмин В.А., Токарев А.Б. Обнаружение и оценка информативности побочных электромагнитных излучений в многофункциональном комплексе радиомониторинга АРК-Д1ТИ. / Специальная техника, 2006, № 2, с. 51 – 56.
4. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы средства. – М.: Горячая линия – Телеком, 2006, с. 492.