ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 621.396.677; 621.397.671

ПРИНЦИПЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ СЛУЧАЙНЫХ АНТЕНН

Заседателева П.С., Маслов О.Н., Рябушкин А.В., Шашенков В.Ф.

Рассматривается возможность активной защиты распределенной случайной антенны (РСА) с помощью аддитивных и мультипликативных помех.

Ключевые слова: активная защита информации, распределенные случайные антенны, аддитивные и мультипликативные преднамеренные помехи

Введение

Для обеспечения защиты конфиденциальной информации (КИ) в коммерческих организациях важное значение имеют выявление и последовательное перекрытие всех технических каналов утечки, в том числе по соединительным линиям (СЛ), отходящим из подлежащих защите помещений (ПЗП) во внешнюю среду [1-3]. Примерами ПЗП являются помещения (служебные кабинеты, переговорные комнаты и кабины, конференц-залы), предназначенные для проведения совещаний, переговоров и конференций менеджерами организации. Излучателями сигналов, содержащих КИ (далее КИ-сигналы), в каналах утечки являются случайные антенны, сосредоточенные и распределенные, анализ и моделирование которых является одним из перспективных направлений развития современной статистической теории антенн [4]. Примерами РСА являются СЛ со сложной и разветвленной (многоэтажной и многоэлементной) структурой – сети электропитания, заземления, оповещения, охранной и пожарной сигнализации; линии внешней, внутриофисной и компьютерной связи; системы труб вентиляции и центрального отопления; металлические части несущих конструкций в зданиях [5].

К негативным особенностям каналов утечки КИ через РСА относятся:

- сложный и часто неоднозначный (заранее непредсказуемый) характер возбуждения, связанный с преобразованием исходного КИ-сигнала в сигналы, расходящиеся по СЛ. Источниками КИ-сигналов могут быть как основные (непосредственно участвующие в обработке, хранении, передаче и приеме КИ) технические средства (ТС), то есть рабочая аппаратура менеджеров организации, так и вспомогательные (не участвующие в указанных процессах, но находящиеся в ПЗП элементы систем электропитания, заземления, сигнализации и связи, ЭВМ, офисное оборудование);
- обычно принципиально разный характер распространения КИ-сигнала внутри ПЗП и КИ-сигналов в СЛ, с помощью которых ТС, размещенные в ПЗП, подключаются к внешнему оборудованию. В результате этого КИ-сигналы могут с малым затуханием уходить через РСА далеко за пределы ПЗП и становиться доступными для потенциального злоумышленника – недобросовестного конкурента, хакера, специалиста коммерческой разведки и др.;
- труднопреодолимые сложности моделирования (математического, физического, компьютерного) источников КИ-сигналов и СЛ, выступающих в роли РСА;
- негативная динамика экологических и эргономических характеристик ПЗП при использовании большинства известных методов и средств ликвидации каналов утечки КИ – приводящих к тепловому, шумовому и электромагнитному загрязнению ПЗП, ухудшению микроклимата (повышение влажности и изменение состава воздуха без вентиляции), снижению уровня естественного геомагнитного фона и т.п. В ряде случаев нежелательными факторами являются также высокая стоимость, вес и габариты оборудования для защиты ПЗП.

Как разновидность случайных антенн [4] РСА в настоящее время исследованы недостаточно. Способы информационной защиты РСА также имеют ряд неизученных особенностей [5-6]. Это объясняется, во-первых, тем, что, в отличие от СЛ, образующих основные каналы связи (по которым КИ-сигналы поступают к «законным» – санкционированным потребителям КИ), благодаря РСА возникают побочные каналы (каналы утечки КИ), по которым КИ-сигналы поступают к несанкционированным потребителям КИ – злоумышленникам. При организации информационной защиты СЛ основных каналов ограничением является отсутствие недопустимых помех для законных потребителей КИ. При защите РСА

данного ограничения не существует, поскольку к ним могут подключаться только злоумышленники.

Во-вторых, наиболее отработанные и надежные способы пассивной защиты СЛ (электромагнитное экранирование, заземление, фильтрация КИ-сигналов) для защиты РСА (например, в виде системы труб) зачастую неприменимы. Поэтому главным средством обеспечения информационной герметичности ПЗП является активная защита КИ – с использованием различного рода преднамеренных (заградительных шумовых, имитационных и т.п.) помех. В-третьих, поскольку КИ-сигналы через РСА способны с малым затуханием уходить далеко за пределы ПЗП, злоумышленник может использовать в своих целях высокоэффективную стационарную аппаратуру. При проектировании системы защиты КИ необходимо учитывать эти обстоятельства и всеми доступными (особенно нестандартными, инновационными) научно-технологическими способами повышать ее универсальность и эффективность. Цель статьи – анализ возможностей, связанных с применением помех мультипликативного типа в интересах повышения эффективности информационной защиты РСА.

Моделирование сигналов и аддитивных помех в РСА

Известны следующие способы активной защиты КИ, основанные на применении сигналов специального вида (преднамеренных помех), призванных энергетическим способом (для маскирующих шумовых помех) или путем нанесения максимального информационного ущерба (для имитирующих помех) «подавить» КИ-сигналы во всех имеющихся и потенциально возможных каналах утечки, чтобы затруднить злоумышленнику перехват и обработку КИ с помощью имеющихся у него ТС:

- линейное зашумление, которое реализуется с помощью шумового генератора, подающего сигнал с уровнем $U_{ш}(t)$ во все подлежащие защите СЛ;

- пространственное зашумление, которое имеет в виду создание в пределах ПЗП электромагнитного поля (ЭМП) со структурой и характеристиками, обеспечивающими защиту КИ от перехвата по каналам электромагнитной утечки;

- кодовое зашумление – применяемое при невозможности использовать другие виды активной защиты, связанные с ЭМП;

- самозашумление, которое является специфическим видом зашумления компьютеров, когда либо стоящие рядом ЭВМ работают так, что ЭМП их КИ-сигналов искажают друг друга, либо один компьютер работает в мультипрограммном режиме, когда обработка перехваченного КИ-сигнала с целью извлечения КИ злоумышленником затруднена.

Перспективным направлением развития методов активной защиты является применение генераторов имитационных помех, способных при малых уровнях ЭМП в окружающем пространстве (что необходимо для обеспечения ЭМС и безопасности условий труда персонала и потребителей КИ) наносить максимальный информационный ущерб потенциальному злоумышленнику. В [7-8] представлены характеристики КИ-сигналов, возникающих при работе ЭВМ разных типов. На основе аналогичных данных для всех ТС, которые могут находиться в ПЗП, были разработаны компьютерные модели сигналов и помех в РСА, сочетающие способы амплитудной и угловой (частотной, фазовой) модуляции, предназначенные для использования при проектировании систем активной защиты КИ [9-10].

Рассмотрим способ линейного зашумления ПЗП. Модель КИ-сигнала в заданной частотно-временной области представляет собой

$$U_c(t) = U_0(t)\cos\Phi(t), \qquad (1)$$

где амплитуда сигнала $U_0(t) = U_A + U_1(t)$; U_A – амплитуда несущей сигнала, $U_1(t)$ – модулирующий амплитуду КИ-сигнал; фазовый угол сигнала $\Phi(t) = \omega_c t + \varphi_c + \Omega_2(t)$; ω_c и φ_c – соответственно, несущая частота и начальная фаза несущей сигнала, $\Omega_2(t)$ – модулирующий фазовый угол КИ-сигнал, t – текущее время.

Идея линейного зашумления состоит в прибавлении к $U_c(t)$ помехи $U_ш(t)$, то есть формирование в СЛ, образующих РСА, аддитивной смеси сигнала и шумовой помехи вида

$$U_c(t) + U_ш(t) = U_0(t)\cos\Phi(t) + U_ш(t). \qquad (2)$$

В принятых обозначениях амплитудной модуляции (АМ) соответствует добавка модулирующего КИ-сигнала $U_1(t)$ к U_A в составе множителя $U_0(t)$; угловой модуляции (УМ) – воздействие $\Omega_2(t)$ на слагаемые в составе углового множителя $\Phi(t)$: при частотной модуляции (ЧМ) – на $\omega_c(t)$; при фазовой модуляции (ФМ) – на $\varphi_c(t)$.

Шумовая помеха $U_ш(t)$ является первым частным случаем реализации аддитивной помехи (АП) $U_{АП}(t)$, которая отвечает условию

$$U(t) = U_c(t) + U_{АП}(t), \qquad (3)$$

где $U(t)$ – сигнал, принимаемый злоумышленником. Вторым частным случаем (3) является применение в качестве $U_{АП}(t)$ вместо $U_ш(t)$ имитирующей помехи $U_и(t)$ – аналогичной по свойствам $U_c(t)$, однако не связанной с модулирующими КИ-сигналами $U_1(t)$ и $\Omega_2(t)$.

Теория приема дискретных сообщений предусматривает обработку аддитивной смеси сигнала и помехи с помощью высокоэффективных помехоустойчивых алгоритмов [11]. Поэтому основным недостатком АП – как при линейном зашумлении с помощью $U_ш(t)$, так и при использовании имитирующих помех $U_и(t)$ – является возможность существенно снизить эффективность информационной защиты РСА путем применения злоумышленником известных методов повышения помехоустойчивости приема сумм (2)-(3) для цифровых сигналов любого конкретного вида. Кроме того, достижение необходимой эффективности защиты РСА требует увеличения $U_ш(t)$ до уровней, представляющих экологическую опасность для окружающей среды по электромагнитному фактору [2].

При использовании имитационных помех $U_и(t)$, аналогичных по параметрам КИ-сигналу, информационный ущерб, наносимый злоумышленнику, зависит от точности воспроизведения помехами параметров КИ-сигналов, которые, одновременно, должны быть лишены конкретного КИ-содержания [12-13]. Эти требования противоречат друг другу, что существенно осложняет возможность реализации данного способа информационной защиты РСА. Применение имитирующих помех затрудняет также необходимость постоянной синхронизации помехи с КИ-сигналом.

При защите РСА, в которых циркулируют КИ-сигналы, сопровождающие работу ЭВМ, основной интерес представляют цифровые виды модуляции ФМ-2 и АМ-2 [12]. Для других ТС в качестве КИ-сигналов могут выступать также сигналы с другими видами УМ (ЧМ и ФМ) [13]. При рассмотрении возможных вариантов перехвата КИ определяют с помощью аналитического расчета или методом компьютерного имитационного моделирования [12-13], как воздействуют АП разного вида на помехоустойчивость приема КИ-сигналов с указанной модуляцией. При этом учитывается, что реальные помехи и КИ-сигналы обычно имеют взаимно перекрывающиеся частотные спектры и соизмеримые по интенсивности уровни.

Анализ показывает, что АП существенно снижают помехоустойчивость приема КИ-сигналов с АМ [11], поэтому они способны обеспечивать требуемую степень информационной безопасности РСА. Однако при наличии в РСА КИ-сигналов с УМ (ФМ и ЧМ) эффективность защиты КИ-сигналов с помощью АП может быть существенно снижена злоумышленником путем обработки (2)-(3) с помощью соответствующих ТС. Поэтому целесообразно рассмотреть и другие варианты разрушения (резкого снижения пропускной способности) каналов утечки КИ.

Моделирование сигналов и мультипликативных помех в РСА

По аналогии с (1)-(3) мультипликативной помехе (МП) $U_{МП}(t)$ соответствует модель

$$U(t) = U_c(t) \cdot k_{МП}(t) \cdot, \qquad (4)$$

где $k_{МП}(t) = \gamma_1 U_{МП}(t)$, γ_1 – коэффициент размерности, который зависит от способа реализации МП. Рассмотрим первый частный случай: когда смесь КИ-сигнала и АП подвергается стохастической АМ с помощью МП $k_{МП}(t)$. При этом в РСА формируется стохастический суммарный КИ-сигнал $U_\Omega(t)\cos\Phi(t) + U_П(t)$, где амплитуда сигнала

$$U_\Omega(t) = U_0(t)\, k_{МП}(t) = \gamma_1 [U_A U_{МП}(t) + U_1(t)\, U_{МП}(t)].$$

Преобразованная АП в данном случае представляет собой $U_П(t) = \gamma_1 U_ш(t)\, U_{МП}(t)$.

Таким образом, вместо модулирующего амплитуду КИ-сигнала $U_1(t)$ при реализации данного способа защиты РСА в суммарном сигнале фигурирует произведение $U_1(t)U_{МП}(t)$, результатом чего является снижение помехоустойчивости приема КИ-сигналов в побочном канале утечки КИ для КИ-сигналов с АМ и УМ (ФМ и ЧМ). Аналогичные явления имеют место при одиночном приеме КИ-сигналов – в отсутствие и при наличии замираний многолучевого сигнала. Однако, в отличие от [11], при стохастической АМ в РСА эти «замирания» создаются искусственно – путем применения МП $k_{МП}(t)$.

Анализ показывает, что МП при АМ (для КИ-сигналов с пассивной паузой) малоэффективны [14], однако при УМ (ФМ и ЧМ) они способны значительно снижать помехоустойчивость приема КИ-сигналов с активной паузой. Поскольку в РСА, подлежащих информационной защите, могут циркулировать КИ-сигналы с АМ и УМ одновременно, на практике целесообразно использовать АП и МП совместно. Тем более что в таком случае применение МП малой мощности допускает снижение мощности АП, что ведет к

повышению экологической чистоты системы информационной защиты РСА по электромагнитному фактору [3] без ущерба для эффективности ее функционирования.

В техническом отношении сущность предлагаемого способа информационной защиты РСА, включающего подключение к ней, наряду с N устройствами сопряжения и генераторами помех, которые обеспечивают информационную защиту РСА, состоит в том, что в состав M из числа N устройств сопряжения вводят $M \le N$ амплитудных модуляторов, которые под воздействием M генераторов помех осуществляют совместную стохастическую АМ информационных сигналов и помех, излучаемых РСА.

Прогнозируемая эффективность применения МП в САЗ РСА

Рис. 1 иллюстрирует лабораторный вариант реализации данного способа защиты РСА, который включает ТС – защищаемое техническое средство (оборудование ПЗП; ЭВМ и т.п.); ПУ – параметрическое устройство, управляемое в точках A-A по параметру $R_{МП}(t)$, – выделено штриховым контуром; УМ – усилитель мощности, с выхода которого на ПУ подается МП вида $U_{МП}(t)$; РТР – разделительный трансформатор сети электропитания 220 В, 50 Гц; РСА – фрагмент сети электропитания 220 В, 50 Гц; ИП – измерительный прибор (осциллограф, анализатор спектра), подключаемый к РСА. На схеме рис. 1 штриховыми линиями условно показано также, что сигнал ГШ через УМ и РТР может непосредственным образом воздействовать на РСА в качестве АП вида $U_{АП}(t)$.

Дадим оценку информационного ущерба для ТСП за счет применения САЗ при внесении в РСА активного сопротивления $R_{МП}(t)$, что эквивалентно стохастической АМ и искусственным замираниям КИ-сигнала под воздействием МП. Согласно [11], при наличии «медленных» относительно длительности элемента КИ-сигнала изменений $R_{МП}(t)$ под воздействием $U_{МП}(t)$ в схеме на рис. 1 помехоустойчивость одиночного приема определяется вероятностью ошибки

$$p_{ош}^{МП} = \int_{z_1}^{z_2} p_{ош}^{0}(z)\, w_1(z)\, dz, \quad z\,[z_1; z_2], \qquad (5)$$

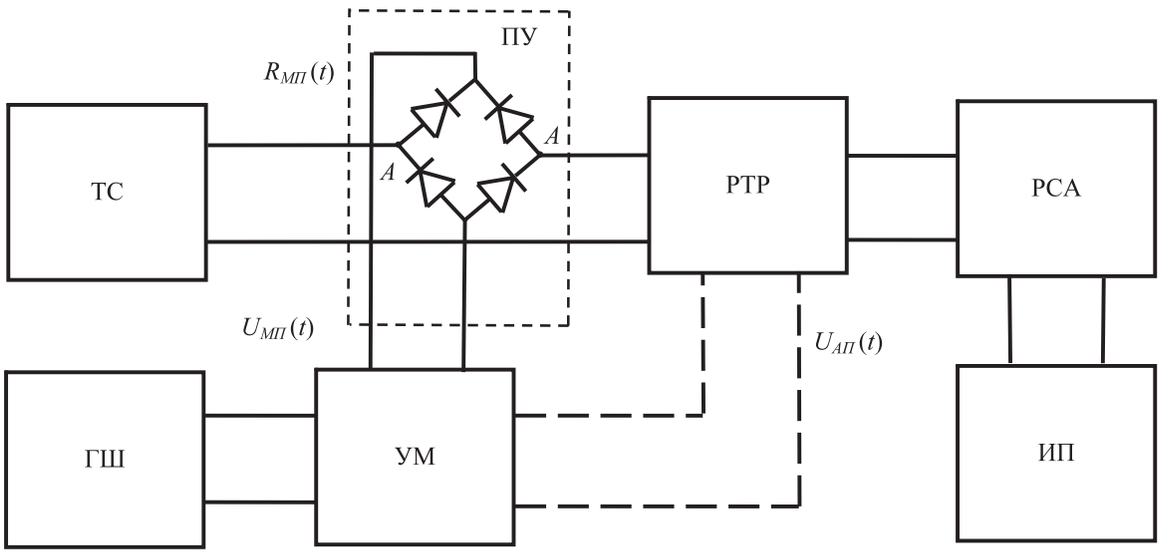


Рис. 1. Схема установки для исследования на универсальном лабораторном стенде эффективности САЗ РСА в виде фрагмента сети электропитания 220 В; 50 Гц

где $p_{ош}^{0}(z)$ – вероятность ошибки при отсутствии МП, далее просто $p_{ош}^{0}$; $w_1(z)$ – плотность распределения вероятности (ПРВ), соответствующая закону изменения коэффициента передачи канала утечки КИ вследствие МП; $z = h^2$ – среднее значение отношения «сигнал/шум». При некогерентном одиночном приеме $p_{ош}^{0} = 0{,}5\exp(-\alpha z)$, где значение α определяется видом модуляции сигнала (для ОФТ $\alpha = 1$; для ЧТ $\alpha = 1/2$), и аналогичным образом при когерентном приеме $p_{ош}^{0} = 0{,}5[1 - \Phi(\sqrt{\alpha z})]$, где $\Phi(\sqrt{\alpha z})$ – функция Крампа [11]. В качестве $w_1(z)$ в [14] рассмотрены равномерный закон $w_1(z) = 1/[z_2 - z_1]$ и усеченный нормальный закон $w_1(z) = A_N^{-1} \exp[-(z - z_0)^2 / 2\sigma^2]$, где z_0 и σ – числовые параметры закона; A_N – коэффициент нормировки в пределах $z\,[z_1; z_2]$.

Рассмотрим следующие три типовых варианта исходных условий для оценки эффективности САЗ РСА при наличии МП путем расчета параметра $\chi_{МП} = p_{ош}^{МП} / p_{ош}^{0}$.

1. Некогерентный прием ОФТ и ЧТ при равномерном законе $w_1(z)$ и $z_1 = k_z z_2$, когда

$$\chi_{МП} = \frac{\exp[\alpha z_2(1-k_z)]-1}{\alpha z_2(1-k_z)} . \quad (6)$$

2. Когерентный прием ОФТ и ЧТ при равномерном законе $w_1(z)$ и $z_1 = k_z z_2$, когда

$$\chi_{МП} = \frac{\pi\{\exp[4\alpha z_2(1-k_z)/\pi]-1\}}{4\alpha z_2(1-k_z)} . \quad (7)$$

3. Некогерентный прием ОФТ и ЧТ при одностороннем нормальном законе и $z_0 = z_2$; $z_1 = k_z z_2$, когда

$$\chi_{МП} = \exp\left(\frac{\sigma^2}{2}\right)\times \times \frac{\Phi\left(\frac{\sigma}{\sqrt{2}}\right) - \Phi\left[\frac{\sigma^2 - z_2(1-k_z)}{\sqrt{2}\,\sigma}\right]}{\Phi\left[\frac{z_2(1-k_z)}{\sqrt{2}\,\sigma}\right]} . \quad (8)$$

Анализ показывает [14], во-первых, что значения «выигрыша» (далее без кавычек) $\chi_{МП}(k_z)$ в помехоустойчивости несанкционированного приема КИ-сигналов, который достигается за счет применения МП в САЗ РСА, для ОФТ ($\alpha = 1$, вариант 1) и ЧТ ($\alpha = 1/2$, вариант 2) отличаются друг от друга только масштабом по оси значений $z = h^2$. Во-вторых, что способ приема КИ-сигнала мало влияет на $\chi_{МП}(k_z)$. Поэтому для более громоздкой формы записи одностороннего нормального закона ограничимся случаем некогерентного приема ОФТ (вариант 3), чтобы оценить влияние неравномерного характера $w_1(z)$ на указанный выигрыш.

Результаты расчетов представлены в таблице 1 в виде зависимостей $\chi_{МП}(k_z)$ для всех трех вариантов, соответствующих (6)-(8). Приводимые рядом в одной строке значения z_2 и $\chi_{МП}^{0,1}$ соответствуют вероятности ошибочного приема КИ-сигнала $p_{ош}^{0} = 0{,}1$; аналогичные значения $\chi_{МП}^{0,01}$ – вероятности $p_{ош}^{0} = 0{,}01$. Параметр одностороннего нормального закона для варианта 3 принят равным $\sigma = \sqrt{2}/2$. Из данных таблицы 1 видно, что, вне зависимости от вида модуляции КИ-сигнала и способа его приема, создаваемые с помощью МП искусственные замирания существенно увеличивают вероятность его ошибочного приема в ТСП. При этом во всех рассматриваемых ситуациях главным фактором эффективного «разрушения» канала утечки КИ-сигнала является расширение динамического диапазона $z\,[z_1; z_2]$ МП, поскольку максимальный выигрыш $\chi_{МП}$ здесь всегда имеет место при $z_1 = 0$ – как при равномерном, так и при неравномерном законе $w_1(z)$.

Таблица 1. Эффективность САЗ РСА при разных вариантах моделирования МП

Вариант	z_2	k_z	0	0,2	0,4	0,6	0,8	1
1	1,61	$\chi_{МП}^{0,1}$	2,49	2,04	1,685	1,40	1,18	1
	3,91	$\chi_{МП}^{0,01}$	12,5	6,99	4,03	2,42	1,15	
2	0,72	$\chi_{МП}^{0,1}$	1,64	1,48	1,33	1,21	1,095	
	2,53	$\chi_{МП}^{0,01}$	7,465	4,72	3,06	2,04	1,41	
3	1,61	$\chi_{МП}^{0,1}$	2,41	2,03	1,62	1,52	1,21	
	3,91	$\chi_{МП}^{0,01}$	9,54	5,94	3,76	2,35	1,49	

Результаты экспериментального исследования изделия «СОМ»

Элементы схемы ГШ; УМ; ПУ и РТР (см. рис. 1) конструктивно объединены в виде изделия «СОМ», являющегося совместной разработкой ПГУТИ и ООО «РЕНОМ» (г. Москва). Тестирование и испытания «СОМ» (далее без кавычек) в лабораторных условиях подтвердили работоспособность и практическую эффективность его применения в составе САЗ РСА. На рис. 2 показана схема подключения СОМ к РСА в виде линии электропитания 220 В; 50 Гц с обозначением трех точек подключения следующих ТС: источника КИ-сигнала и нагрузки, в качестве которой в разных сочетаниях использовались генераторы Г4-143; Г4-116 и монитор ЭВМ SAMSUNG SyncMaster 753DFX, а также ИП (см. рис. 1), роль которого выполняли анализатор спектра FS300 производства Rodhe&Schwarz и осциллограф АКИП 4113/2. Экспериментальные данные, соответствующие разным вариантам реализации схемы на рис. 2, представлены на рис. 3-7.

На рис. 3 приведены спектрограммы смеси КИ-сигнала и сигнала СОМ (при включенном

ГШ, верхние графики), циркулирующих в РСА, которая представляет собой фрагмент линии электропитания 220 В; 50 Гц длиной 12 м на частотах до 100 МГц. Нижние графики на рис. 3 (при отключенном ГШ) соответствуют уровню фона по ЭМП в помещении лаборатории. Сигнал, создаваемый СОМ и генератором Г4-143, размещенным на месте нагрузки и подключенным к СОМ в точке *2*, снимался с РСА при помощи кольцевого ферромагнитного съемника и многовиткового *L*-съемника в точке *3* («на входе» РСА) и в точке *1* («на выходе» РСА). Данный вариант реализации схемы на рис. 2 соответствует прямому однократному прохождению КИ-сигнала через СОМ и для практики является основным.

Из верхних графиков на рис. 3 видно, во-первых, что в сеть электропитания 220 В; 50 Гц напрямую проходит шумовая АП $U_{АП}$ (t), создаваемая ГШ изделия СОМ (см. рис. 1) – интенсивности которой вполне хватает для маскировки КИ-сигнала с частотой 25 МГц и недостаточно для КИ-сигнала с частотой 40 МГц. Во-вторых, что от способа съема сигнала в цепи электропитания мало что зависит: спек-

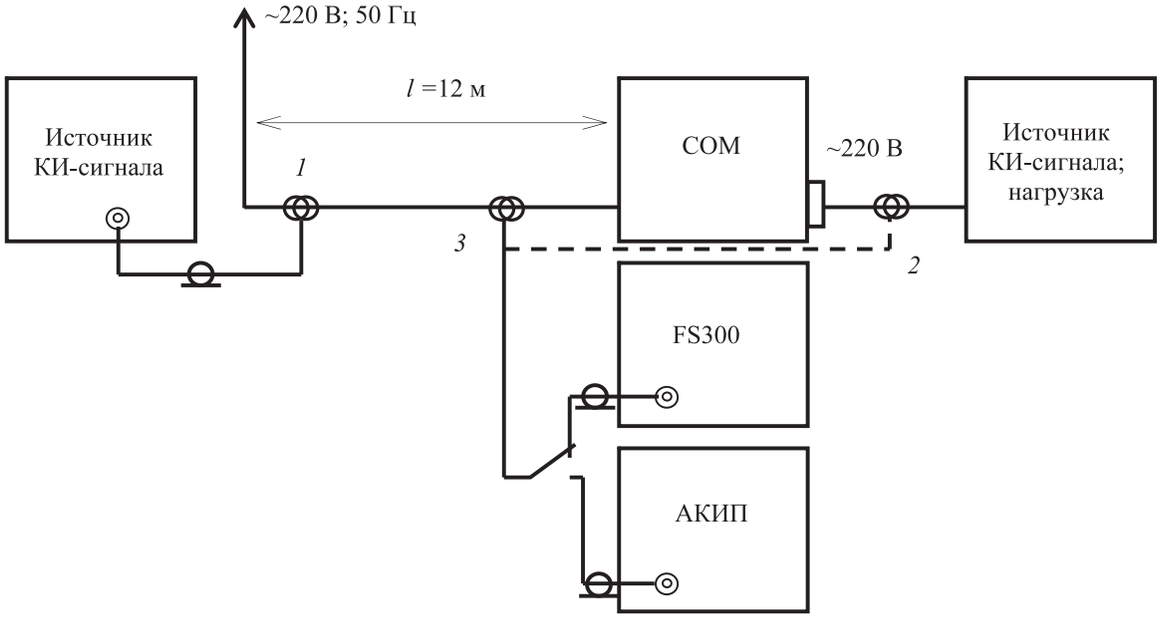


Рис. 2. Схема подключения СОМ к РСА в виде линии электропитания 220 В; 50 Гц и его экспериментального исследования

тры при ферритовом съемнике и при *L*-съемнике близки по форме.

В-третьих, можно отметить также, что удаление точки наблюдения на l = 12 м по сравнению со стандартной точкой l = 1 м несколько меняет соотношение между уровнями КИ-сигнала и шумовой АП на частоте 40 МГц, однако это различия невелики. В-четвертых, что достигаемое за счет работы изделия СОМ отношение «помеха/сигнал» в РСА больше зависит от частоты, чем от расстояния.

Осциллограммы, соответствующие данному основному варианту реализации схемы на рис. 2 (генератор Г4-143 на месте нагрузки, АКИП в точке 1), показаны на рис. 4. При разных периодах развертки 5 мс … 1 мкс по осциллограммам отчетливо видно, что гармонический тестовый КИ-сигнал с частотой 25 МГц в РСА за счет работы СОМ подвергается воздействию МП в виде стохастической АМ.

Обратное прохождение КИ-сигнала через СОМ (однократное и двойное) иллюстрируют спектрограммы на рис. 5 и осциллограммы на рис. 6. Данный вариант реализации схемы на рис. 2 соответствует расположению генератора Г4-143 в точке *1* при размещении в точке *2* при однократном прохождении и в точке *3* при двойном прохождении, соответственно, анализатора

FS300 и осциллографа АКИП, в качестве нагрузки использован генератор Г4-116.

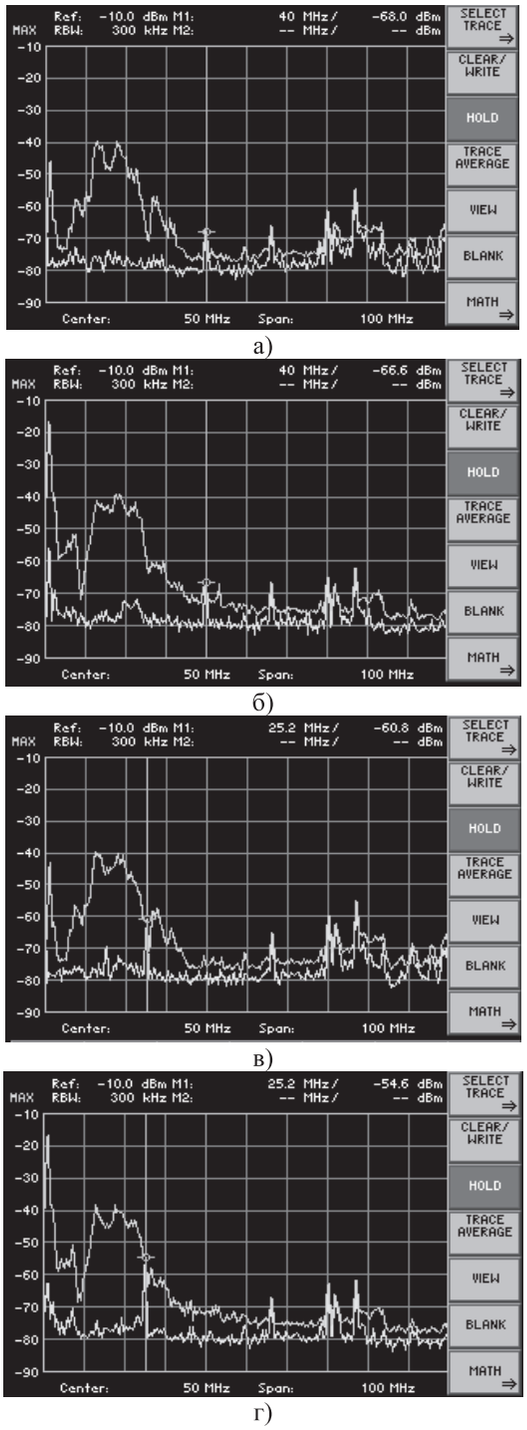


Рис. 3. Спектрограммы смеси КИ-сигнала и сигнала COM для РСА в виде линии электропитания 220 В; 50 Гц, на частотах до 100 МГц; источник КИ-сигнала – генератор Г4-143, частота 40 МГц (а-б) и 25 МГц (в-г), на расстоянии l = 12 м от COM при отключенном ГШ (нижние графики) и включенном ГШ (верхние графики); а;в) индуктивный L-съемник; б;г) ферритовый съемник; а-б) частота КИ-сигнала 40 МГц; в-г) частота КИ-сигнала 25 МГц

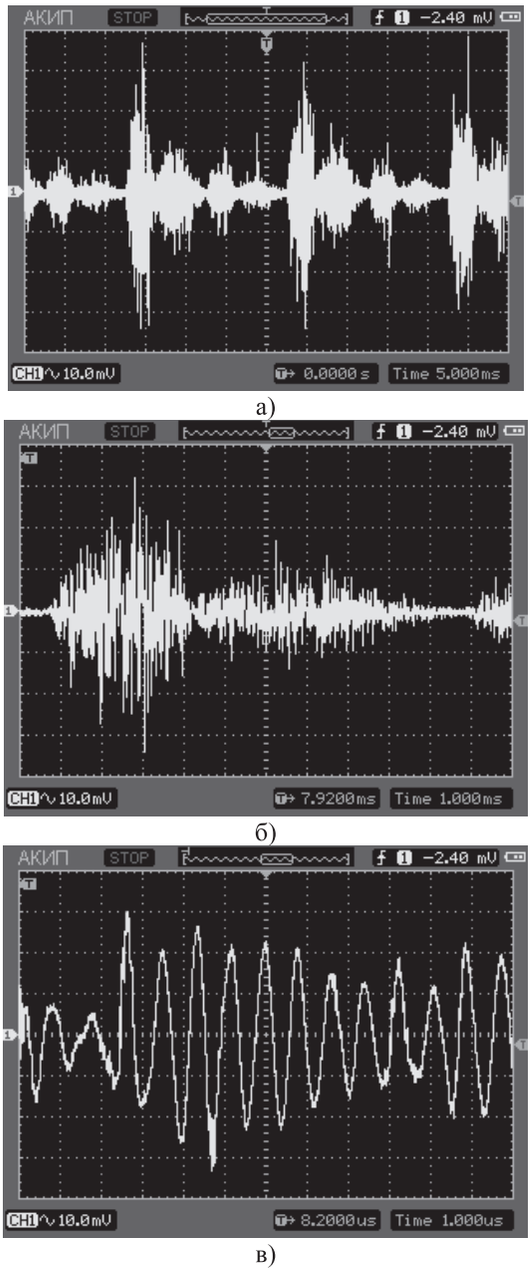
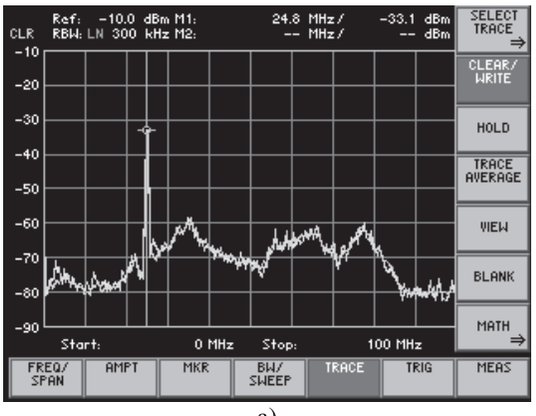
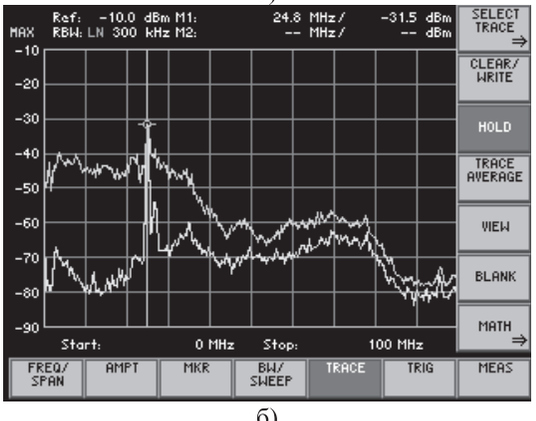


Рис. 4. Осциллограммы смеси КИ-сигнала с частотой 25 МГц и сигнала COM для РСА в виде линии электропитания при периоде развертки:
а) 5 мс; б) 1 мс; в) 1 мкс

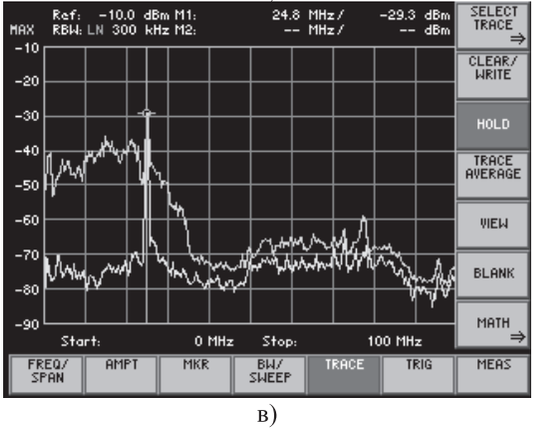
Данные рис. 5-7 показывают, во-первых, что при отключенной от COM нагрузке сигнал от его ГШ в сеть электропитания в качестве АП не проходит и на тестовый КИ-сигнал (см. графики рис. 5а-7а) не воздействует; во-вторых, что КИ-сигнал после прохождения COM (как однократного, так и двойного) в обратном направлении эффективно «разрушается» за счет стохастической АМ в виде шумовых импульсов. Это говорит о целесообразности применения COM для устранения каналов утечки КИ, формируемых с помощью метода «высокочастотного навязывания» [1-2], что имеет важное самостоятельное значение.



а)

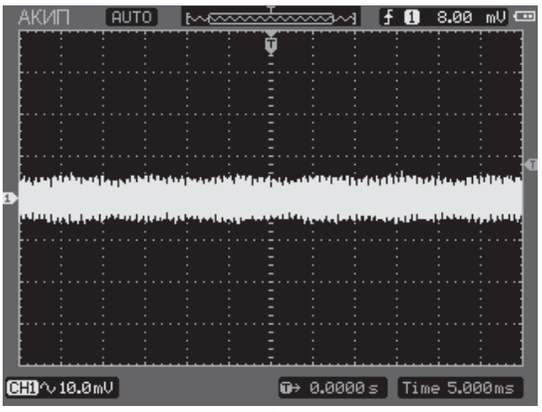


б)

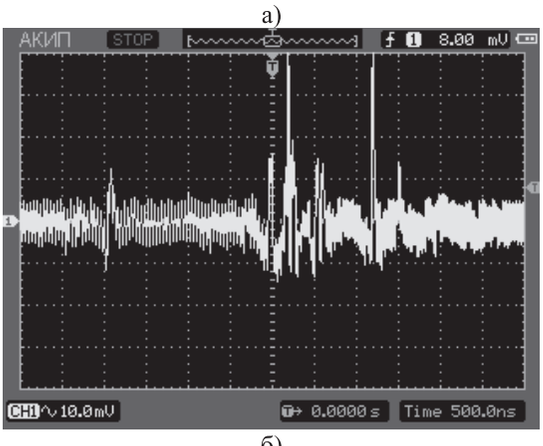


в)

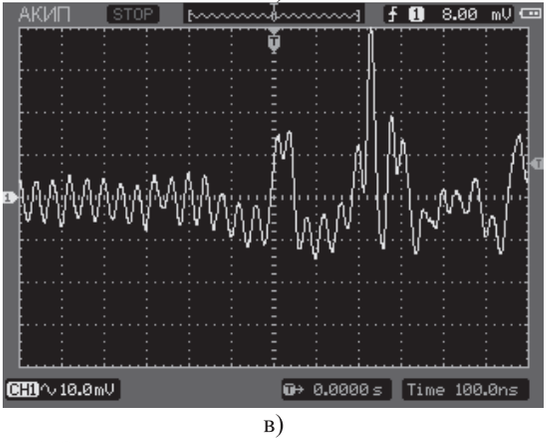
Рис. 5. Спектрограммы смеси КИ-сигнала с частотой 25 МГц и сигнала СОМ: а) ГШ отключен; б-в) ГШ и нагрузка подключены; б) однократное прохождение; в) двойное прохождение



а)



б)



в)

Рис. 6. Осциллограммы смеси КИ-сигнала с частотой 25 МГц и сигнала СОМ при обратном однократном прохождении: а) ГШотключен; б-в) ГШ и нагрузка подключены; б) период развертки 500 нс; б) 100 нс

Выводы

Для повышения эффективности защиты КИ, циркулирующей в РСА, наряду с маскирующими шумовыми и прицельными имитирующими АП предлагается использовать преднамеренные МП, изменяющие коэффициент передачи РСА. Воздействие МП эквивалентно применению АМ и УМ стохастического типа, существенно снижающих пропускную способность побочных каналов утечки КИ, возникающих в РСА.

Результаты экспериментального исследования изделия СОМ, реализующего предложенный способ информационной защиты РСА, показали его высокую эффективность и перспективность практического применения для защиты цепей электропитания ЭВМ и других ТС. В теоретическом плане актуальной задачей является анализ эффективности применения МП с помощью метода статистического имитационного моделирования, учитывающего неопределенности условий работы реальных РСА. В практическом отношении представляет интерес разработка модификаций СОМ для защиты цепей заземления, сигнализации, управления и других СЛ, отходящих из ПЗП во внешнюю среду.

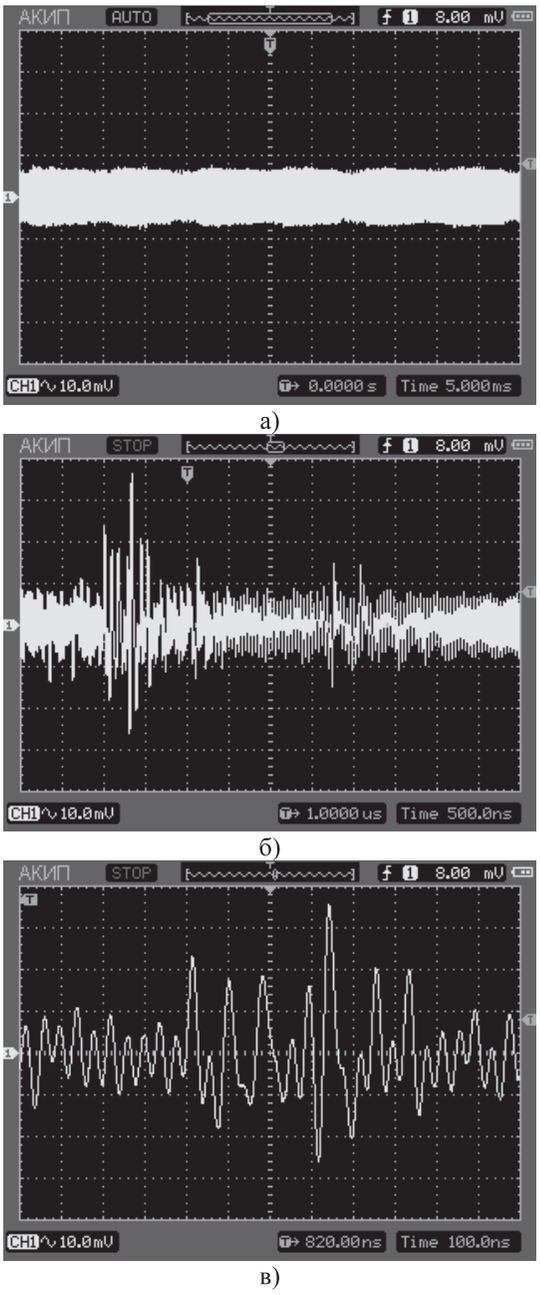


Рис. 7. Осциллограммы смеси КИ-сигнала с частотой 25 МГц и сигнала COM при обратном двойном прохождении: а) ГШ отключен; б-в) ГШ и нагрузка подключены; б) период развертки 500 нс; б) 100 нс

Литература

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. М.: Гостехкомиссия России, 1998. – 320 с.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – Телеком, 2005. – 416 с.
3. Маслов О.Н., Шашенков В.Ф. Защита информации: аспект электромагнитной совместимости и безопасности // Вестник связи. 2005. №2. – С. 65-72.
4. Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Методы и средства исследования эффективности случайных антенн // Антенны. №4 (131), 2008. – С. 59-65.
5. Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Оценка эффективности распределенных случайных антенн // Антенны. №10 (149), 2009. – С. 62-69.
6. Способ определения затухания сигнала в распределенной случайной антенне // Маслов О.Н., Раков А.С., Рябушкин А.В. Патент RU 2 393 493 C1 от 06.04.2009, опубл. 27.06.2009, бюлл. №18.
7. Маслов О.Н., Соломатин М.А., Васильевский А.Д. Тестовые сигналы для анализа ПЭМИН персональных ЭВМ // ИКТ. Т.5, №2, 2007. – С.79-82.
8. Маслов О.Н., Соломатин М.А., Егоренков В.Д. Тестовые сигналы для анализа ПЭМИН периферийных устройств персональных ЭВМ // ИКТ. Т.5, №2, 2007. – С.82-84.
9. Способ оценки эффективности случайной антенны // Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Патент RU 2372623 от 03.03.2008, опубл. 10.11. 2009, бюлл. №31.
10. Способ определения параметров случайной антенны // Алышев Ю.В., Маслов О.Н., Рябушкин А.В. Патент RU 2374655 от 10.01.2008, опубл. 27.11. 2009, бюлл. №33.
11. Финк Л.М. Теория передачи дискретных сообщений. М.: Сов. радио, 1970. – 728 с.
12. Алышев Ю.В., Маслов О.Н. К оценке эффективности случайных антенн по критерию информационного ущерба // ИКТ. Т.6, №3, 2008. – С. 116-125.
13. Алышев Ю.В., Маслов О.Н. Тестирование модели измерительного комплекса для исследования случайных антенн // ИКТ. Т.7, №1, 2009. – С. 67-72.
14. Маслов О.Н., Щербакова Т.А. Анализ и моделирование мультипликативных процессов // Радиотехника. №6, 2012. – С. 101-105.

INFORMATION SECURITY PRINCIPLES OF DISTRIBUTED RANDOM ANTENNAS

Zasedateleva P.S., Maslov O.N., Ryabushkin A.V., Shashenkov V.F.

The capability of active protection of distributed random antennas with additive and multiplicative noise is considered in this paper.

Keywords: *active information protection, distributed random antennas, additive and multiplicative jamming.*

Заседателева Полина Сергеевна, аспирант Кафедры экономических и информационных систем (ЭИС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-917-117-83-86

Маслов Олег Николаевич, д.т.н., профессор, заведующий Кафедрой ЭИС ПГУТИ. Тел. 8-902-371-06-24. E-mail: maslov@psati.ru

Рябушкин Аркадий Викторович, инженер Кафедры «Мультисервисные сети и информационная безопасность» ПГУТИ. Тел. (8-846) 339-11-43. E-mail: ryabushkin@psati.ru

Шашенков Валерий Федорович, к.т.н., с.н.с., соискатель Кафедры ЭИС ПГУТИ. Тел. 8-903-144-50-75. E-mail: maslov@psati.ru

УДК 621.396.677; 621.397.671

АНАЛИЗ И МОДЕЛИРОВАНИЕ СИГНАЛОВ В СИСТЕМЕ ИНФОРМАЦИОННОЙ ЗАЩИТЫ РАСПРЕДЕЛЕННОЙ СЛУЧАЙНОЙ АНТЕННЫ

Заседателева П.С., Маслов О.Н., Рябушкин А.В., Шашенков В.Ф.

Рассматривается проблема моделирования сигналов и активных преднамеренных помех, используемых в системе информационной защиты распределенной случайной антенны (РСА).

Ключевые слова: активная защита информации, распределенные случайные антенны, используемые сигналы и помехи

Введение

Как разновидность случайных антенн (см. классификацию [1]) распределенные случайные антенны (РСА) изучены в настоящее время недостаточно полно. Способы защиты конфиденциальной информации (КИ), утечка которой из подлежащих защите помещений (ПЗП) может происходить через РСА, также имеют ряд неисследованных особенностей [2-4]. Это объясняется целым рядом причин, основными из которых являются:

- сложный и часто непредсказуемый характер возбуждения РСА, связанный с преобразованием исходного КИ-сигнала в сигналы, расходящиеся по соединительным линиям (СЛ), образующим РСА. Источниками КИ-сигналов могут быть как основные (непосредственно участвующие в обработке, хранении, передаче и приеме КИ) технические средства (ТС), так и вспомогательные (не участвующие в указанных процессах, но находящиеся в подлежащем защите помещении (ПЗП) устройства: ЭВМ, офисное оборудование и т.п.; фрагментами РСА являются СЛ систем электропитания, заземления, сигнализации и связи;

- существенно разный характер распространения КИ-сигналов внутри ПЗП и в СЛ, образующих РСА, – с помощью которых ТС, размещенные в ПЗП, подключаются к внешнему оборудованию и по которым КИ-сигналы могут с малым затуханием уходить за пределы ПЗП и становиться доступными для злоумышленника – недобросовестного конкурента, специалиста коммерческой разведки и др.;

- труднопреодолимые сложности моделирования (математического, физического, компьютерного) источников КИ-сигналов и СЛ, выступающих в роли РСА;

- негативная динамика эколого-эргономических характеристик ПЗП при использовании большинства известных методов и средств ликвидации каналов утечки КИ через РСА, приводящих к удорожанию оборудования, необходимого для информационной защиты ПЗП;

- невозможность использовать отработанные и надежные способы пассивной защиты СЛ (электромагнитное экранирование, заземление, фильтрация КИ-сигналов) для защиты РСА (например, в виде системы труб или металлических конструкций здания), ввиду чего главным средством обеспечения информационной герметичности ПЗП является активная защита КИ – с использованием различного рода преднамеренных (заградительных шумовых, имитационных и т.п.) помех;

- возможность использования злоумышленником за пределами ПЗП высокоэффективной стационарной аппаратуры для обработки КИ-сигналов, которые с малым затуханием «транспортируют» ему туда РСА и т.д.

Важное значение для проектирования систем защиты КИ имеют анализ и моделирование сигналов и помех, циркулирующих в РСА, которые состоят из СЛ со сложной и разветвленной (многоэтажной и многоэлементной) структурой – таких, как сети электропитания, заземления, оповещения, охранной и пожарной сигнализации; линии внешней, внутриофисной и компьютерной связи; системы труб вентиляции и центрального