твенного рынка программного обеспечения для бизнеса занимают системы, автоматизирующие именно функцию учета (оперативного, бухгалтерского и налогового). Поэтому в преставлении многих отечественных предпринимателей и руководителей основные бизнес-процессы неоправданно и, как правило, безотчетно отождествляются с процессами учета.

Управленческая функция контроля реализуется на уровне производственных операций, то есть на достаточно детальном уровне. Поэтому оставим процессы контроля на нижних уровнях декомпозиции и перейдем к реализации управленческой функции анализа.

Анализ процессов управления, реализующих функцию анализа для подразделения

Анализ проводится для извлечения определенных выводов с целью принятия решений и выработки рекомендаций. По этой причине его логично проводить по итогам реализации одного или нескольких циклов бизнес-процессов. Поэтому разместим процессы анализа после основных бизнес-процессов. Пример такого способа размещения представлен на рис. 4. Внесение процессов анализа на первый уровень декомпозиции позволяет анализировать состав отчетов, которые будут формироваться по ходу производственной деятельности и обсуждать состав данных, которые необходимо аккумулировать на уровне каждого из основных бизнес-процессов.

Выводы

Таким образом, предложенный методический подход позволяет отображать и анализировать процессы управления уже на первом уровне декомпозиции основных производственных процессов предприятия. Это даст возможность снизить затраты на разработку технического задания при внедрении КИС, глубже понять взаимосвязь основных процессов с процессами управления; приведет к повышению качества и эффективности управления всей системы в целом.

Литература

1. Кознов Д.В. Основы визуального моделирования. М: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 246 с.
2. Глушков И.Е. Бухгалтерский учет на предприятиях различных форм собственности. М.: КНОРУС; Новосибирск: ЭКОР-КНИГА, 2008. – 994 с.
3. Трошин Ю.В. Сравнительный анализ методов описания бизнес-процессов // Тезисы XVI РНК ПГУТИ, январь, 2009. – С. 251-252.
4. Маклаков С.В. Моделирование бизнес-процессов с AllFusion PM. М.: Изд. Диалог-МИФИ, 2007. – 224 с.

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК. 621.395.4

ТЕСТИРОВАНИЕ МОДЕЛИ ИЗМЕРИТЕЛЬНОГО КОМПЛЕКСА ДЛЯ ИССЛЕДОВАНИЯ СЛУЧАЙНЫХ АНТЕНН

Алышев Ю. В., Маслов О. Н.

В статье представлены результаты тестирования компьютерной модели измерительного комплекса, предназначенного для исследования случайных антенн (СА) методом статистического имитационного моделирования (СИМ) с применением критерия относительного информационного ущерба.

Введение

При проектировании и анализе эффективности систем активной защиты (САЗ) информации [1-2] с применением компьютерного метода СИМ [3-5] важное значение имеет адекватность СИМ-модели измерительного комплекса (ИК), предназначенного для оценки относительного информационного ущерба, обусловленного работой САЗ. При цифровой передаче конфиденциальной информации (КИ) оценка указанного ущерба сводится к вычислению вероятности ошибки $P(\text{ош}) = N_{\text{ош}} / N_0$, где $N_{\text{ош}}$ и N_0 – число ошибочно принятых символов и общее число символов, принятых ИК.

Моделью источника КИ является многоканальная СА (сосредоточенная или распределенная), сигналы в каналах которой (КИ-сигналы) соответствуют как основному, так и побочным реальным каналам утечки КИ [2; 6]. Считается, что

элементы САЗ способны создавать как шумовые (заградительные, маскирующие), так и имитационные (прицельные) преднамеренные помехи – в последнем случае идентичные по своим параметрам КИ-сигналам, но не содержащие КИ.

В отличие от [3-5], где СИМ-модель ИК определялась для случая использования в СА максимально эффективных способов передачи и приема КИ, в настоящей статье, во-первых, рассматриваются КИ-сигналы, близкие по свойствам сигналам в реальных каналах утечки КИ – возникающим, например, при работе персональных ЭВМ [7-8]. Во-вторых, для тестирования СИМ-модели ИК выбран одноканальный режим работы СА, где аналитические выражения $P(\text{ош})$ известны [9-10].

Модели КИ-сигналов

Будем считать, что КИ-сигналами в рассматриваемой одноканальной СА являются сигналы фазовой (ФМ-2) и амплитудной (АМ-2) двоичной модуляции. После перехвата данные сигналы, согласно [9], могут быть обработаны и демодулированы известными способами. Для противодействия этому в состав САЗ вводятся генераторы шума (ГШ), благодаря которым на входе ИК уменьшается отношение «сигнал-шум». В итоге даже при оптимальной демодуляции КИ сигналов вероятность $P(\text{ош})$ в ИК резко возрастает.

Однако применение ГШ с требуемой мощностью излучения имеет ряд негативных последствий: ухудшаются электромагнитная совместимость и безопасность рабочего оборудования, использование разнесенного приема в ИК позволяет снизить $P(\text{ош})$ и т. д. Поэтому необходимо рассмотреть варианты совместного использования ГШ и генераторов имитационных помех (ГП) разного вида, соответствующих сигналам АМ-2 и ФМ-2.

Таким образом, представляют интерес 4 варианта реализации СИМ-модели рассматриваемой системы «СА-ГШ-ГП-ИК», соответствующие 4 разным сочетаниям КИ-сигнала и помехи: ФМ-2/ФМ-2; ФМ-2/АМ-2; АМ-2/ФМ-2; АМ-2/АМ-2.

По аналогии с [3-5] введем обозначения моделируемых КИ-сигналов: $S_{\text{СФМ-2}}(t)$ при ФМ-2 и $S_{\text{САМ-2}}(t)$ при АМ-2, и помех: $S_{\text{ПФМ-2}}(t)$ при ФМ-2 и $S_{\text{ПАМ-2}}(t)$ при АМ-2. Сигнал на входе ИК при этом имеет вид $z(t) = S_{\text{С}}(t) + S_{\text{П}}(t) + n(t)$, где $n(t)$ соответствует сигналу ГШ. Тогда в рамках СИМ-модели для двоичных сигналов и помех:

– при ФМ-2 в $S_{\text{СФМ-2}}(t)$ «0» соответствует 1, «1» соответствует –1;
– при АМ-2 в $S_{\text{САМ-2}}(t)$ «0» соответствует 0, «1» соответствует 1;
– при ФМ-2 в $S_{\text{ПФМ-2}}(t)$ «0» соответствует a, «1» соответствует $-a$;
– при АМ-2 в $S_{\text{ПАМ-2}}(t)$ «0» соответствует 0, «1» соответствует a.

Вероятность появления символа «0» в КИ-сигнале P_0; вероятность символа «1» – P_1. Аналогичные вероятности для помех (в которых КИ отсутствует) примем равными $P_0' = P_1' = 0,5$ (штрих вверху означает, что этот параметр характеризует помеху). Согласно [9], уровень порога принятия решения в одно-лучевом канале для АМ-2 равен 0,5; для ФМ-2 – 0.

Результаты расчета *P* (ош)

Рассматриваемые 4 варианта реализации ИК обозначим следующим образом:

– ФМ-2/ФМ-2;
– ФМ-2/АМ-2;
– АМ-2/ФМ-2;
– АМ-2/АМ-2. (1)

Общая вероятность ошибки в ИК для каждого варианта будет определяться суммой

$$P(\text{ош}) = P_{00}(\text{ош}) + P_{01}(\text{ош}) + P_{10}(\text{ош}) + P_{11}(\text{ош}), \quad (2)$$

где нижние индексы соответствуют передаваемым символам полезного и мешающего сигналов.

Рассмотрим поочередно каждый вариант сочетания КИ-сигнала и помехи, определив для него значение переменной *z* и вероятности ошибки.

Данную схему иллюстрирует рис. 1, на котором в условном виде показаны кривая распределения плотности вероятности шума *w*(*z*), а также сигналы $S_{\text{СФМ-2}}(t)$; $S_{\text{САМ-2}}(t)$; $S_{\text{ПФМ-2}}(t)$ и $S_{\text{ПАМ-2}}(t)$, а область значений аргумента *z*, соответствующая событию ошибки, заштрихована. Для каждого из 4 вариантов формирования суммы КИ-сигнала и помехи согласно (1) возможны 4 варианта суммирования двоичных сигналов «0» и «1».

Для первого варианта ФМ-2/ФМ-2 при $S_{\text{СФМ-2}}(t)$ = «0» для КИ-сигнала и ФМ-2 «0» для помехи (см. рис. 1а) в (2) при этом получаем

$$P_0: \quad z = 1 + a + n; \; P_{00}(\text{ош}) = P_0' P_0 Q(1 + a);$$

при ФМ-2 «0» для КИ-сигнала и ФМ-2 «1» для помехи (см. рис. 1б)

$$P_0: \quad z = 1 - a + n; \; P_{01}(\text{ош}) = P_1' P_0 Q(1 - a);$$

при ФМ-2 «1» для КИ-сигнала и ФМ-2 «0» для помехи (см. рис. 1в)

$$P_1: \quad z = -1 + a + n; \; P_{10}(\text{ош}) = P_0' P_1 Q(1 - a);$$

при ФМ-2 «1» для КИ-сигнала и ФМ-2 «1» для помехи (см. рис. 1г)

$$P_1: \quad z=-1-a+n;\ P_{11}(\text{ош})=P_1'P_1Q(1+a)$$

где $Q(z)$ – функция ошибок [10].

Вариант для $a>1$, приведенный на рис. 1 д, соответствует варианту, приведенному на рис. 1 б для $a\le 1$. В итоге вероятность ошибки для первого варианта

$$\begin{aligned}P(\text{ош})&=P_0'P_0Q(1+a)+P_1'P_0Q(1-a)+\\&+P_0'P_1Q(1-a)+P_1'P_1Q(1+a)=\\&=0,5\cdot(P_0+P_1)\big(Q(1+a)+Q(1-a)\big)=\\&=0,5\cdot\big(Q(1+a)+Q(1-a)\big).\end{aligned}\tag{3}$$

Аналогичным образом для второго варианта ФМ-2/АМ-2 получаем при ФМ-2 «0» для КИ-сигнала и АМ-2 «0» для помехи

$$P_0: \quad z=1+0+n=1+n;\ P_{00}(\text{ош})=P_0'P_0Q(1);$$

при ФМ-2 «0» для КИ-сигнала и АМ-2 «1» для помехи

$$P_0: \quad z=1+a+n;\ P_{01}(\text{ош})=P_1'P_0Q(1+a);$$

при ФМ-2 «1» для КИ-сигнала и АМ-2 «0» для помехи

$$P_1: \quad z=-1+0+n=-1+n;\ P_{10}(\text{ош})=P_0'P_1Q(1);$$

при ФМ-2 «1» для КИ-сигнала и АМ-2 «1» для помехи

$$P_1: \quad z=-1+a+n;\ P_{11}(\text{ош})=P_1'P_1Q(1-a).$$

Вероятность ошибки для второго варианта:

$$\begin{aligned}P(\text{ош})&=P_0'P_0Q(1)+P_1'P_0Q(1+a)+P_0'P_1Q(1)+\\&+P_1'P_1Q(1-a)=0,5\times\\&\times\Big((P_0+P_1)Q(1)+0,5\cdot\big(P_0Q(1+a)+P_1Q(1-a)\big)\Big)=\\&=0,5\cdot Q(1)+0,25\big(Q(1+a)+Q(1-a)\big).\end{aligned}\tag{4}$$

Для третьего варианта АМ-2/ФМ-2 при АМ-2 «0» для КИ-сигнала и ФМ-2 «0» для помехи

$$P_0: z=0+a+n=a+n;\ P_{00}(\text{ош})=P_0'P_0Q(0,5-a);$$

при АМ-2 «0» для КИ-сигнала и ФМ-2 «1» для помехи

$$P_0: z=0-a+n=n-a;\ P_{01}(\text{ош})=P_1'P_0Q(0,5+a);$$

при АМ-2 «1» для КИ-сигнала и ФМ-2 «0» для помехи

$$P_1: \quad z=1+a+n;\ P_{10}(\text{ош})=P_0'P_1Q(0,5+a);$$

при АМ-2 «1» для КИ-сигнала и ФМ-2 «1» для помехи

$$P_1: \quad z=1-a+n;\ P_{11}(\text{ош})=P_1'P_1Q(0,5-a).$$

Вероятность ошибки для третьего варианта:

$$\begin{aligned}P(\text{ош})&=P_0'P_0Q(0,5-a)+P_1'P_0Q(0,5+a)+\\&+P_0'P_1Q(0,5+a)+P_1'P_1Q(0,5-a)=\\&=0,5\cdot(P_0+P_1)\big(Q(0,5-a)+Q(0,5+a)\big)=\\&=0,5\cdot\big(Q(0,5-a)+Q(0,5+a)\big).\end{aligned}\tag{5}$$

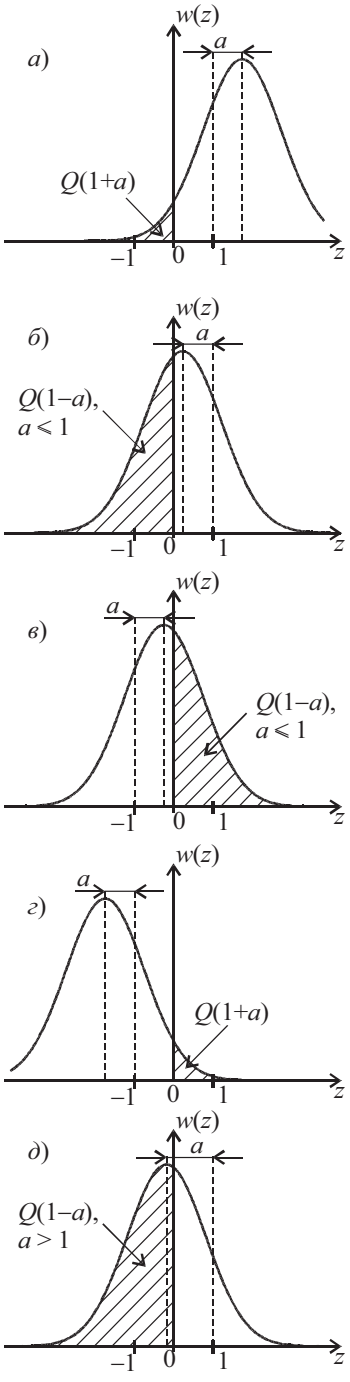

Рис. 1. К определению вероятности ошибки $P(\text{ош})$ для первого варианта ФМ-2/ФМ-2

Для четвертого варианта АМ-2/АМ-2 при АМ-2 «0» для КИ-сигнала и АМ-2 «0» для помехи

$$P_0: \quad z = 0+0+n = 0+n;\ P_{00}(\text{ош}) = P_0' P_0 Q(0,5);$$

при АМ-2 «0» для КИ-сигнала и АМ-2 «1» для помехи

$$P_0: z = 0+a+n = a+n;\ P_{01}(\text{ош}) = P_1' P_0 Q(0,5-a);$$

при АМ-2 «1» для КИ-сигнала и АМ-2 «0» для помехи

$$P_1: \quad z = 1+0+n = 1+n;\ P_{10}(\text{ош}) = P_0' P_1 Q(0,5);$$

при АМ-2 «1» для КИ-сигнала и АМ-2 «1» для помехи

$$P_1: \quad z = 1+a+n;\ P_{11}(\text{ош}) = P_1' P_1 Q(0,5+a).$$

Вероятность ошибки для четвертого варианта

$$\begin{aligned} P(\text{ош}) &= P_0' P_0 Q(0,5) + P_1' P_0 Q(0,5-a) + \\ &+ P_0' P_1 Q(0,5) + P_1' P_1 Q(0,5+a) = \\ &= 0,5 \cdot (P_0 + P_1) Q(0,5) + \\ &+ 0,5 \cdot \left(P_0 Q(0,5-a) + P_1 Q(0,5+a)\right) = \\ &= 0,5 Q(0,5) + 0,25\left(Q(0,5-a) + Q(0,5+a)\right). \end{aligned} \qquad (6)$$

Результаты расчета по формулам (3)-(6) представлены на рис. 2а-г в виде сплошных линий. Графики рис. 2а соответствуют первому рассматриваемому варианту: ФМ-2 для КИ-сигнала и ФМ-2 для помехи; рис. 2б – второму варианту: ФМ-2 для КИ-сигнала и АМ-2 для помехи; рис. 2в – третьему варианту: АМ-2 для КИ-сигнала и ФМ-2 для помехи; рис. 2г – четвертому варианту: АМ-2 для КИ-сигнала и АМ-2 для помехи. Расчетные кривые 1 на рис. 2 соответствуют отношению уровней «сигнал/помеха», равному 0,1; графики *2* – 0,5; графики *3* – 1,0; графики *4* – 2,0; графики *5* – 4,0; графики *6* – 10,0. Расчетные данные рис. 2 позволяют провести тестирование разработанной СИМ-модели ИК для исследования СА.

Результаты моделирования

При проведении СИМ процесса приема и обработки в ИК совокупности вышеуказанных сигналов и помех объем выборки для каждой точки кривой на рис. 2 составлял 16777239 переданных информационных символов. Тестовый сигнал представлял собой один период *m*-последовательности длиной $16777216 = 2^{24}$ символов и дополнительно 23 нулевых символа в конце, а мешающий сигнал – псевдослучайную последовательность из 1677239 символов.

Выходные данные СИМ, показанные на кривых рис. 2 утолщенными точками, отличаются от расчетных значений в 3-4 знаке после запятой. Это говорит о том, что результаты тестирования СИМ-модели ИК для частного случая одноканальной СА при использовании КИ-сигналов и помех с ФМ-2 и АМ-2 хорошо подтверждаются путем расчета по известным аналитическим формулам. Поэтому предложенная в [3-5] СИМ-модель ИК может применяться и в более сложных общих случаях: для исследования с помощью метода СИМ многоканальных СА с другими видами модуляции КИ-сигналов и помех.

Выводы

При проектировании САЗ для предотвращения утечки КИ по основному и побочным каналам в СА [1-2; 6], наряду с ГШ целесообразно применять ГП. Использование в интересах САЗ прицельных помех, идентичных КИ-сигналам, но не содержащих КИ, позволяет даже при значительных отношениях уровней «сигнал/шум» и оптимальном способе демодуляции сигналов в ИК обеспечить $P(\text{ош}) = 0,5$. Данные СИМ позволяют предположить, что, независимо от вида модуляции ИК-сигналов, вид модуляции ФМ-2 в ГП является наиболее предпочтительным.

Результаты тестирования разработанной СИМ-модели ИК [2; 4-5] позволяют рекомендовать ее для применения при исследования методом СИМ других, более сложных вариантов реализации многоканальных СА. Исходными данными для «запуска» СИМ-модели ИК являются энергетические характеристики полезного сигнала, прицельной и шумовой помех, полученные в результате СИМ конкретных вариантов реализации СА – как сосредоточенных, так и распределенных.

Литература

1. Электромагнитная безопасность и имитационное моделирование инфокоммуникационных систем. Под ред. Маслова О.Н. М.: Радио и связь, 2002. – 288 с.
2. Алышев Ю.В., Маслов О.Н., Раков А.С., Рябушкин А.В. Исследование случайных антенн методом статистического имитационного моделирования // Успехи современной радиоэлектроники. №7, 2008. – С. 3-41.
3. Маслов О.Н., Раков А.С., Шашенков В.Ф, Яруллин Н.Т. Эффективность САЗ побочного электромагнитного канала утечки информации: постановка задачи и описание объекта СИМ // ИКТ. Т.3, №3, 2005. – С. 65-72.

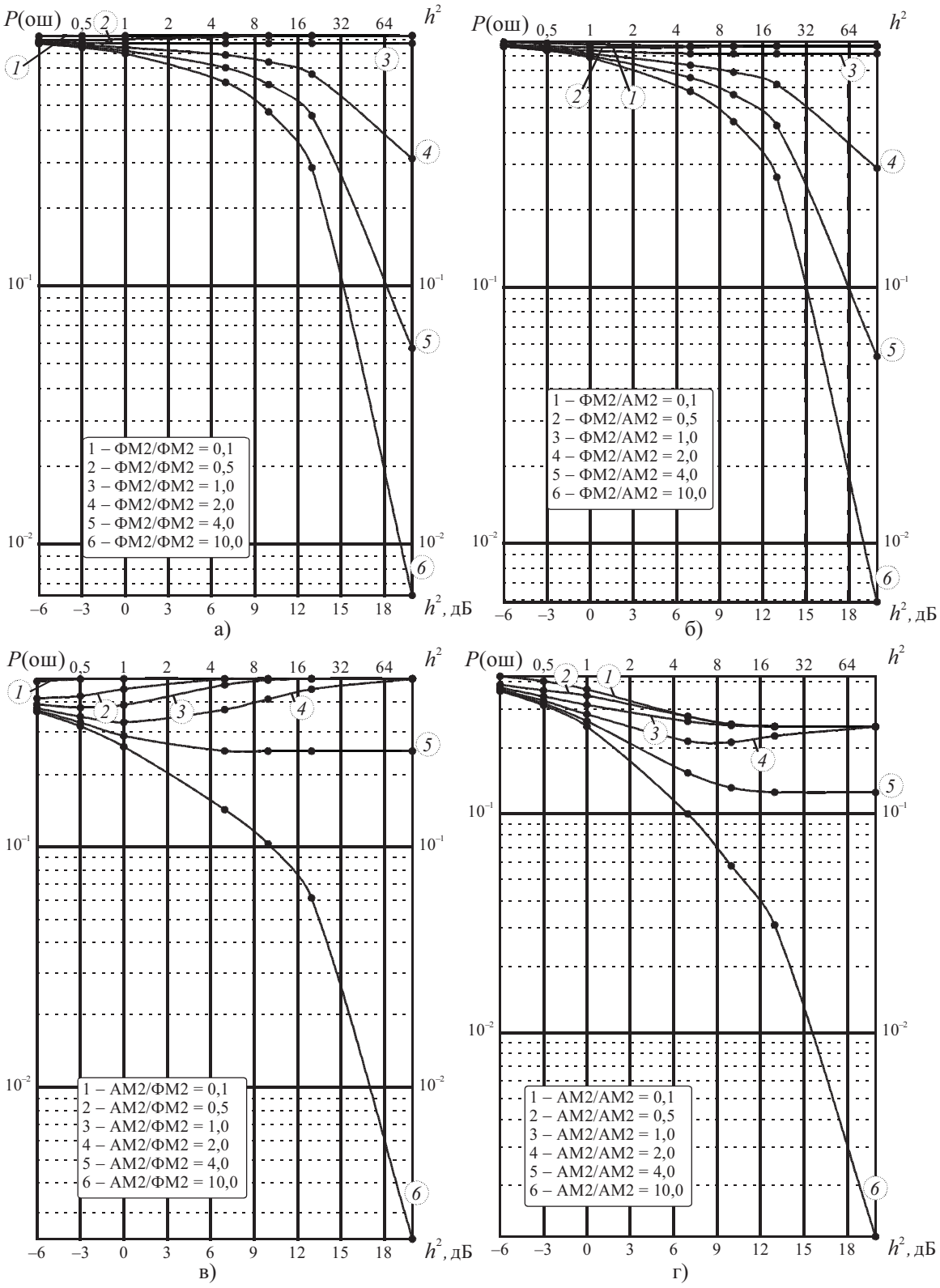

Рис. 2. Зависимость вероятности ошибки $P(\text{ош})$ от отношения «сигнал-шум» h^2, дБ при фиксированных отношениях «сигнал-помеха» (кривые *1*: $S_{\text{СМ-2}} / S_{\text{ПМ-2}} = 0{,}1$; *2* – 0,5; *3* – 1,0; *4* – 2,0; *5* – 4,0; *6* – 10,0), варианты а) – ФМ-2/ФМ-2; б) – ФМ-2/АМ-2; в) – АМ-2/ФМ-2; г) – АМ-2/АМ-2

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. Применение технологии MIMO для исследования случайных антенн // Радиотехника. №3, 2008. – С. 61-65.
6. Маслов О.Н., Рябушкин А.В. Сотовые терминалы: утечка информации по интермодуляционным каналам // Мобильные телекоммуникации. №6, 2008. – С. 11-14.
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. Финк Л.М. Теория передачи дискретных сообщений. М.: Сов. радио, 1970. – 728 с.
10. Возенкрафт Д., Джекобс И. Теоретические основы радиотехники и связи: Пер. с англ. под ред. Р. Л. Добрушина. М.: Мир, 1969. – 640 с.

УДК: 519.72

ИСПОЛЬЗОВАНИЕ ЗАКОНА РАСПРЕДЕЛЕНИЯ ХИ-КВАДРАТ ДЛЯ АНАЛИТИЧЕСКОГО ОПИСАНИЯ СТАТИСТИК БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ

Захаров О.С., Иванов А.И.

В статье рассматривается проблема аппроксимации распределений параметров реальных биометрических образов из тестовых баз. Показано, что минимальную ошибку дает нормированное хи-квадрат распределение, которое может использоваться при сертификации систем аутентификации по тайным рукописным паролям.

Механизмы дистанционной высоконадежной биометрической аутентификации пользователей могут использоваться для защиты различных систем от несанкционированного доступа, либо проверки авторства при электронном документообороте. Созданные макеты (биометрико-нейросетевые контейнеры) по заверениям производителей обладают стойкостью к атакам подбора равной 10^{-12}. Данные характеристики должны быть подтверждены статистическим тестированием на реальных данных. Очевидно, что сбор баз реальных биометрических примеров, необходимых для тестирования высоконадёжных систем, потребует огромного времени и затрат [1]. Высокая надежность – это высокий размер тестовых баз. Таким образом, появляется потребность в механизмах, позволяющих оценивать стойкость высоконадежных биометрико-нейросетевых систем на сокращенных выборках. Так, зная закон распределения значений биометрических данных, можно существенно сократить число тестовых примеров для получения «качественной» оценки. Для этого надо осуществить классификацию параметров и добиться нужной представительности тестовой выборки в каждом из подклассов.

При формировании больших баз тестовых образов можно классифицировать вводимые образы по группам стабильности, уникальности и качества их параметров [2]. Таким образом, для каждого образа из базы тестовых образов должны быть указаны средняя стабильность, средняя уникальность и среднее качество всех биометрических параметров данного образа. Далее встаёт проблема выбора закона, позволяющего описывать распределение параметров стабильности, уникальности и качества с максимальной достоверностью.

Описание преобразователей биометрии пользователя в код доступа строится с использованием классических законов распределения значений. Например, для оценки стойкости средства аутентификации к атакам подбора используется биномиальный закон, а для проверки гипотезы закона совместного распределения биометрических параметров – хи-квадрат распределение. Классические варианты этих законов построены на предположении независимости входных параметров [3]. Получаемые с их помощью оценки оказываются завышенными для случая реальных (зависимых между собой) биометрических данных. Для получения более достоверных статистических оценок необходимо при описании распределений биометрических параметров использовать классические законы распределений, имеющие аналитическое описание.

При аппроксимации симметричных эмпирических распределений выборок хорошо под-