"пустого" канала ниже порога обнаружения аппаратуры противника. Необходимо постоянно совершенствовать методы построения скрытых каналов по мере увеличения вычислительной мощности поисковой аппаратуры противника.

Список литературы

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации / Под ред. Ю.С. Ковтанюка. – К.: Издательство Юниор, 2003. – 504с.

2. *Bassia, P., Pitas, I.*: Robust audio watermarking in the time domain. In: Proc. EUSIPCO 98, vol. 1. Rodos, Greece. IEE (1998), P. 25–28.

3. *Swanson, M.D., Zhu, B., Tewfik, A.H., Boney, L.* Robust audio watermarking using perceptual masking. Signal Processing 66 (1998), P. 337–355.

4. *Gruhl, D., Lu, A., Bender, W.* Echo hiding. In: Anderson, R. (ed.): Information Hiding, Cambridge, UK. Lecture Notes in Computer Science, Vol. 1174. Springer-Verlag, Berlin/ Heidelberg (1996) , P. 295–315.

5. *Kirovski D., Malvar H.* Robust Covert Communication over a Public Audio Channel Using Spread Spectrum. Information Hiding Workshop, Pittsburgh, PA, (2001).

6. *Cachin C.* An Information-Theoretic Model for Steganography // Proceeding of the Workshop on Information Hiding. 1998.

7. *Zollner J., Federrath H., Klimant H.* Modeling the security of steganographic systems, 2nd Workshop on Information Hiding: April 1998, Portland, LNCS 1525, Springer Verlag, P. 345-355.

8. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография – М.: СОЛОН-Пресс, 2002.

9. *Provos N.* Defending Against on Statistical Steganalysis // Proceeding of the 10 USENIX Security Symposium. 2001. P. 323–335.

10. *Katzenbeisser S., Petitcolas F.* Defining Security in Steganographic Systems, Proceedings of the SPIE vol. 4675, Security and Watermarking of Multimedia Contents IV, 2002, P. 50-56.

Поступила 25.09.2006

УДК 681.3.06

Степанов В.Д, Хорошко В.А.

ПРИМЕНЕНИЕ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КОРПОРАТИВНЫХ РЕСУРСАХ

Одной из основных задач при создании систем активной защиты (САЗ) является могокритериальная оптимизация оперативно-технических характеристик. Решение этой задачи предусматривает помимо количественного или качественного описания каждой характеристики, их сравнение с аналогичными характеристиками САЗ, использующих другие классы помех. Поэтому оценку их эффективности будем производить путем сравнения соответствующих технических характеристик.

Рассмотрим маскирующую способность прицельной помехи и ее зависимость от параметров, определяющих схемные и конструктивные особенности генераторов помех. Маскирующие свойства прицельной помехи в значительной степени обусловлены таким параметром, как число уровней квантования m. На рис. 1 и 2 приведены результаты расчетов средней вероятности ошибки для последовательных кодов с основанием n и равновероятным

распределением символов [1]. Случай, когда n=2, соответствующий двоичному коду, представляет особый интерес.

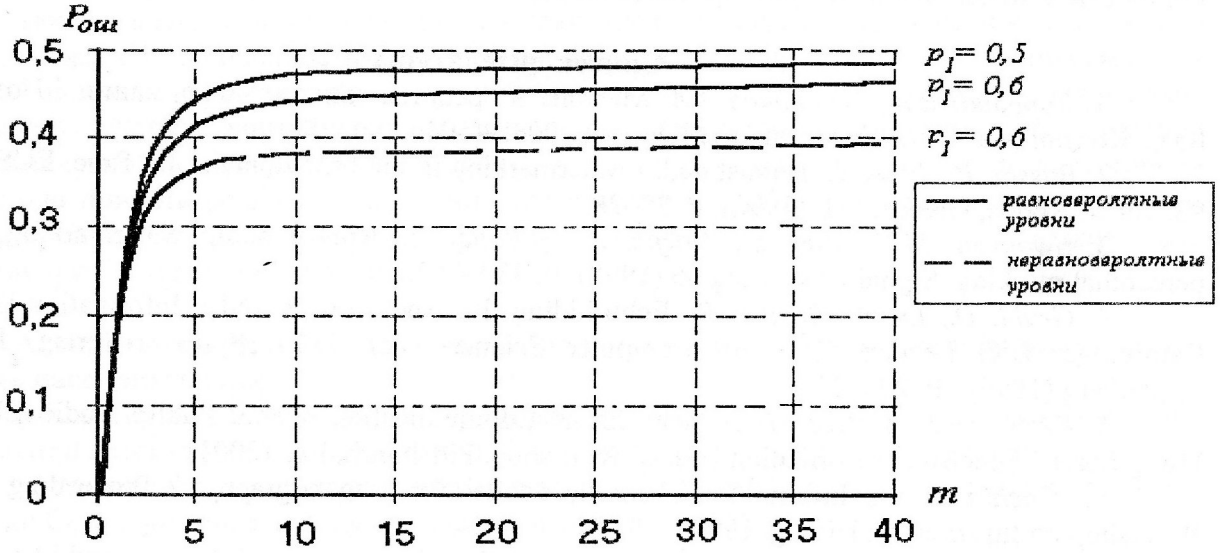

Рис. 1. Зависимость вероятности ошибки от числа уровней квантования помехи

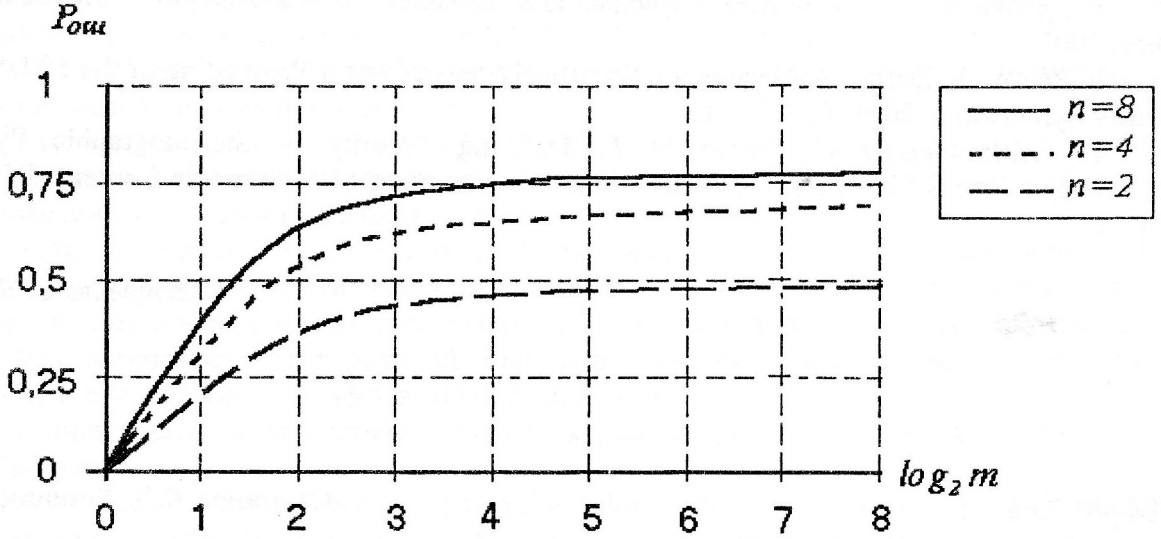

Рис. 2. Зависимость вероятности ошибки от числа уровней квантования помехи для n-ичного последовательного кода с биноминальным распределением уровней

Как видно из рис. 1 нормированная величина вероятности ошибки даже для объектов первой категории ($P_{ош}$ = 0,4602) достигается при относительно небольших величинах параметра m [2, 3].

Рассмотрим маскирующую способность прицельной помехи по отношению к идеальному параллельному коду. Его особенностью является то, что при приеме даже в отсутствии помех возникают ошибки, вероятность которых увеличивается с увеличением разрядности кода. Так, например, уже 8-разрядный параллельный код удовлетворяет требованиям норм по третьей категории [2, 4]. Кроме того, необходимое число уровней квантования помехи в значительной степени зависит от разрядности параллельного кода,

однако, для вероятности ошибки, соответствующей нормам для объектов первой категории, такая зависимость проявляется в меньшей степени.

Сравнение маскирующей способности прицельной и имитирующей помех в условиях полного совпадения параметров помехи и сигнала без учета гауссовского компонента сводится к рассмотрению влияния числа уровней квантования помехи m на среднюю вероятность ошибки.

Предельно допустимая маскирующая способность имитирующей помехи несколько выше, чем у прицельных помех, что доказано экспериментально С другой стороны, маскирующая способность имитирующих помех снижается за счет того, что генератор помех в процессе ее формирования сам становится источником опасного инверсного сигнала и должен проходить специальные исследования. Указанное обстоятельство ограничивает применимость САЗ с имитирующими помехами.

Чем выше разрядность кода, тем больше максимальное число уровней квантования имитирующей помехи m. Для прицельных помех имеет место обратная зависимость числа уровней квантования m от разрядности кода N (рис. 3). Учитывая, что параллельный способ передачи информации является наиболее распространенным в ЭВМ, можно утверждать, что по величине параметра m прицельные помехи дают, в общем случае, выигрыш по сравнению с имитирующими помехами.

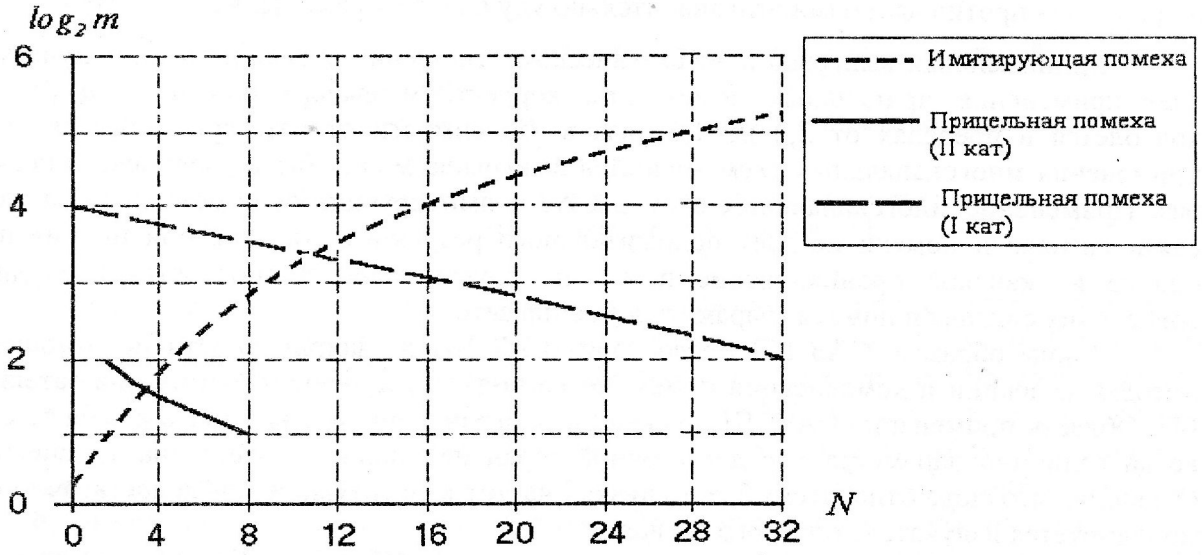

Рис. 3. Зависимость $\log_2 m$ от разрядности параллельного кода для имитирующей и прицельной помех

Таким образом, сравнение прицельных и имитирующих помех по величине маскирующей способности оказывается в пользу первого класса помех. Следует отметить, что прицельные помехи по величине маскирующей способности имеют некоторое преимущество и перед гауссовскими помехами за счет того, что одна и та же средняя вероятность ошибки достигается при меньшей мощности помехи [3]. Более подробно этот вопрос будет рассмотрен при сравнении энергетических показателей.

Рассмотрим количественные показатели защищенности по отношению к методам селекции и компенсации САЗ, использующих сигналоподобные помехи, поскольку для них эта проблема наиболее актуальна. Степень возможной компенсации помех определяется величиной взаимной энергии E или производного от нее параметра - отношения сигнал-помеха/шум q. Иногда удобно пользоваться более сложным параметром η, равным

$$\eta = \frac{E_{Si}}{\sqrt{E_S \cdot E_i}} = \frac{q_{Si}}{\sqrt{q_S \cdot q_i}}. \qquad (1)$$

Для прицельных помех параметр η представляет собой коэффициент корреляции случайного процесса на выходах линейных частей тракта обработки сигнала и канала компенсации помехи.

Воспользуемся результатами, полученными в [1], которые дают возможность проанализировать влияние параметра η на вероятность ошибки.

Для прицельных (m = 15) и имитирующих помех в качестве дополнительного параметра в семействе кривых фигурирует отношение сигнал/шум q_s. Предполагается, что отношение сигнал/шум q_s и помеха/шум q_i равны. Такое предположение вполне корректно, поскольку при практической реализации САЗ стремятся добиться максимального совпадения параметров разряда помехи и сигнала, а имеющиеся несовпадения в основном вызваны незначительными временными задержками и другими различиями временных параметров.

Таким образом, величина отношения сигнал/шум в канале утечки определяет своеобразный допуск на точность параметров как прицельной, так и имитирующей помехи. Параметр m, в основном, влияет на максимальную величину вероятности ошибки.

Снижение вероятности ошибки в канале с имитирующими помехами вызвано тем, что по мере уменьшения взаимной энергии, как известно, фактически улучшается различение сигнала и помехи [3]. Так, например, при η=0 сигнал и помеха становятся ортогональными, а при η = -1- противофазными, что значительно улучшает их различение.

Минимальный выигрыш в энергетическом отношении сигнал/помеха, получаемый за счет применения прицельных помех, при корректном выборе параметра η (η > 0,8) колеблется в пределах от 2,2 до 1,6 раза в зависимости от категории объекта. За счет применения многоканальных схем величина выигрыша может быть увеличена в несколько раз. Применение многоканальных схем в САЗ с имитирующими помехами из-за жесткой связи сигнала и помехи не дает положительного результата, так как при приеме помехи одного из каналов проникновение помех из других каналов способствует ухудшению совпадения сигнала и помехи (параметр η уменьшается).

Таким образом, САЗ ПП превосходят САЗ ИП по защищенности по отношению к методам селекции и компенсации помех, но несколько уступают по этому показателю САЗ ГП. Область применения САЗ ИП должна быть ограниченной и включать в себя те случаи, когда величина параметра η с достаточной гарантией поддерживается на уровне 0,8-0,9. Очевидно, что сюда относится область низких частот и те ситуации, когда достаточно просто моделируется излучатель опасного сигнала.

Сравнение параметров САЗ, характеризующих ЭМС, целесообразно проводить путем анализа влияния относительных энергозатрат (отношения сигнал/помеха q) на величину средней вероятности ошибки. На рис. 4 приведен график, характеризующий зависимость средней вероятности ошибки от отношения сигнал/помеха для канала с $\lambda = 1$.

Кривая, соответствующая прицельной помехе с компенсированной постоянной составляющей, проходит выше кривых, соответствующих как гауссовской, так и прицельной помехе без компенсации постоянной составляющей. Это свидетельствует о том, что прицельная помеха позволяет получать в канале большую вероятность ошибки по сравнению с другими помехами при одинаковой с ними мощности помех. Однако разница в затратах энергии на получение определенной вероятности ошибки для всех трех типов помех неодинакова в различных условиях: для области относительно больших значений $P_{ош}$ соответствующих требованиям норм для объектов первой категории, эта разница невелика, но она становится существенной для области, соответствующей нормам для объектов второй и третьей категорий.

При рассмотрении канала с неравновероятным появлением единиц и нулей, что менее характерно для опасных сигналов корпоративных сетей, можно отметить те же тенденции. В этом случае придельные помехи с равновероятными и неравновероятными уровнями практически на всей шкале измерений отношения сигнал/помеха превосходят гауссовские помехи.

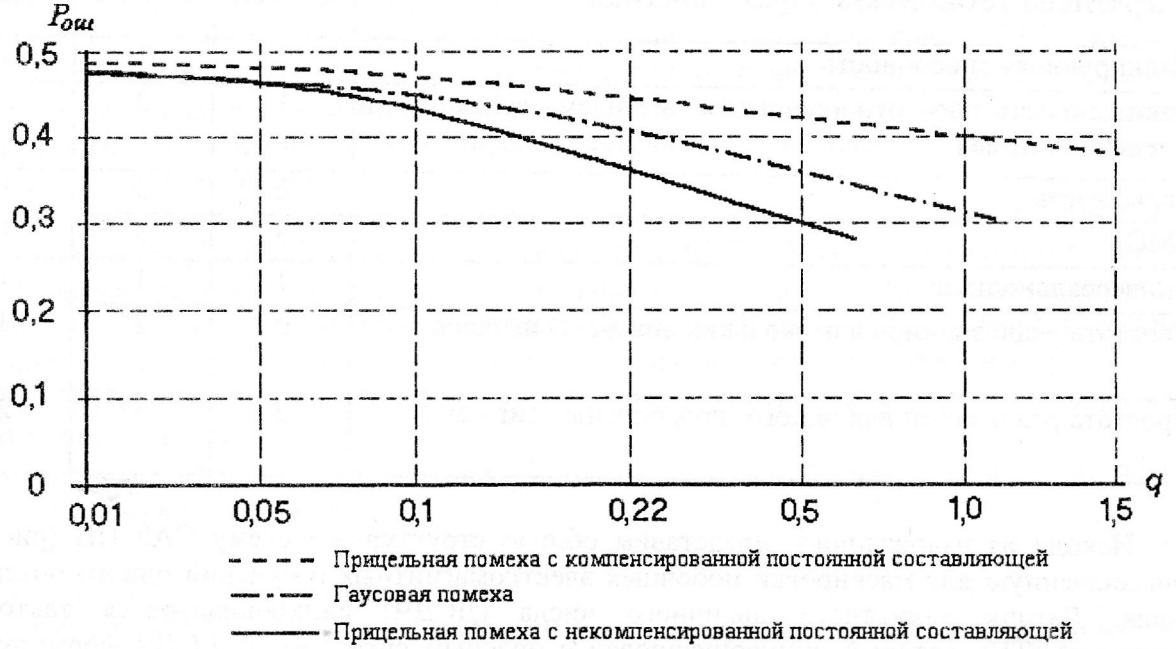

Рис. 4. Вероятностно-энергетические характеристики прицельных и гауссовских помех для λ= 1

Представляет определенный интерес сравнение прицельных помех с равновероятными и неравновероятными уровнями квантования друг с другом. Прицельные помехи с неравновероятными уровнями даже при больших m имеют ограниченную мощность, вызванную тем, что вероятность больших уровней стремится к нулю. Однако и вероятность ошибки для этих помех стремится к некоторому пределу, связанному с величиной λ, который меньше соответствующего предела вероятности ошибки в канале с помехой, имеющей равновероятные уровни. Это объясняется особенностью работы оптимального приемного устройства для прицельных помех с неравновероятными уровнями [3]. Таким образом, прицельная помеха с равновероятными уровнями превосходит аналогичную помеху с неравновероятными уровнями квантования по всем показателям, включая простоту реализации.

Обобщенные результаты качественного и количественного анализа основных оперативно-технических характеристик САЗ, использующих прицельные, имитирующие и гауссовские помехи, проведенного в данном разделе, приведены в табл. 1. Экспертная оценка отдельных показателей осуществлялась по 3-балльной ранжированной.системе.

В табл. 1 маскирующая способность имитирующих помех оценена несколько ниже, чем для других помех, из-за ухудшения специальных свойств вследствие наличия жесткой связи их с информационным сигналом. Скрытность САЗ ПП признана максимальной потому, что помимо сигналоподобного характера помехи, учитывается сложность алгоритма перехвата.

Таким образом, по результатам сравнительного анализа наиболее эффективными следует признать САЗ ПП и, несколько в меньшей степени, САЗ ГП. САЗ ИП уступает им по

общей эффективности и имеет значительно худшие показатели по первым двум важнейшим оперативно-техническим характеристикам.

Таблица 1.
Сравнительная таблица основных оперативно-технических характеристик САЗ

Оперативно-технические характеристики	САЗ ИП	САЗ ПП	САЗ ГП
Маскирующая способность	2	3	3
Защищенность по отношению к методам селекции и компенсации помех	1	2	3
Скрытность	2	3	1
ЭМС	3	3	1
Универсальность	1	1	3
Простота реализации для нескольких опасных сигналов	2	2	3
Простота реализации для одного-двух опасных сигналов	3	3	2

Исходя из изложенного, представим общую структурную схему САЗ ПП (рис. 8), предназначенную для маскировки побочных электромагнитных излучений одного опасного сигнала. Датчик случайного двоичного числа (ДСДЧ) синхронизируется тактовым генератором (ТГ), который синхронизирован с опасным сигналом. В ДСДЧ формируется случайное двоичное число разрядности *m*. Затем это число поступает в регистр сдвига (РС), осуществляющий его последовательное продвижение одновременно с прохождением опасным сигналом различных блоков защищаемого устройства. В результате каждое из сформированных ДСДЧ двоичных чисел последовательно поступает на блоки ключей ($БК_1$,..., $БК_l$), имитирующих излучение опасного сигнала.

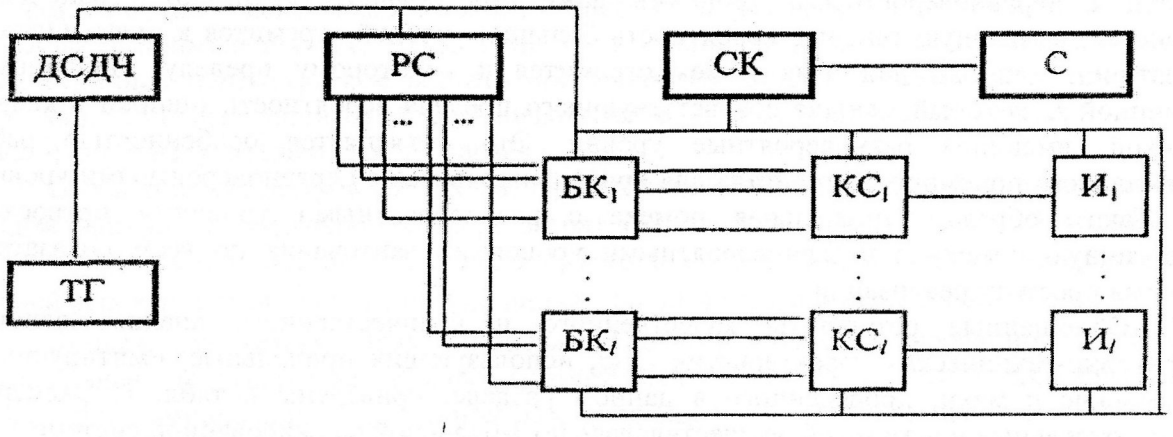

Рис. 5. Структурная схема одноканальной САЗ ПП

Коммутаторы и сумматоры ($БС_1$,..., $БС_l$), производят суммирование разрядов помехи для того, чтобы создать квантованную по случайному закону смесь. Излучатели ($И_1$,...,$И_l$) осуществляют излучение в канал сформированной помехи. Система контроля (СК) обеспечивает проверку работоспособности САЗ и в случае неисправности включает аварийную сигнализацию (С). Благодаря цифровой структуре САЗ ПП, в них легко может быть применен метод борьбы с накоплением опасного сигнала в результате регулярного

повторения информации. С этой целью в ДСДЧ включается буферный регистр, в котором хранится одно из значений случайного двоичного числа в течение всего времени повторения информации. При смене информации происходит изменение числа в буферном регистре, а, следовательно, и реализация помехи, излучаемой в канал утечки. САЗ ПП реализуется в основном на той же элементной и конструктивной базе, что и защищаемое устройство. Генератор размещается, как правило, на отдельной плате, а излучатель монтируется либо на отдельной плате, либо на корпусе устройства.

КПД генератора прицельной помехи существенно превышает КПД генератора гауссовской помехи, требующего высококачественного аналогового усилителя мощности. При этом габариты генератора помех за счет высокого КПД блока формирования помехи и возможности применения современных интегральных микросхем незначительны по сравнению с аналоговыми генераторами.

Быстродействие генератора прицельной помехи в основном связано с быстродействием ДСДЧ. Обычно случайное число в ДСДЧ образуется в результате подсчета числа превышения некоторого уровня, близкого к нулевому, случайным аналоговым процессом. За счет многократного переполнения, средняя частота работы счетчика, связанная с полосой шума, должна быть значительно выше тактовой частоты сигнала. Оценим ограничения, которые накладываются на верхнюю частоту спектра случайного аналогового процесса, F_B.

Воспользовавшись результатами [1] и [2] получим оценку для верхней частоты спектра аналогового шума F_B.

$$F_B > 2 \cdot \sqrt{3} \cdot m \cdot F_T, \qquad (2)$$

где F_T - тактовая частота опасного сигнала.

Согласно (2) для помехи с параметром m=15 верхняя частота спектра аналогового шума, используемого при его формирования по последовательной схеме, должна приблизительно превышать тактовую частоту. Для достижения большего быстродействия следует использовать параллельные методы формирования случайного двоичного числа.

Описав структурную схему САЗ ПП, сформулируем некоторые общие требования к отдельным параметрам таких систем, вытекающие из предыдущего рассмотрения.

Маскирующая способность в значительной степени определяется числом уровней квантования помехи m. В зависимости от того, для решения каких задач предназначено защищаемое ТС, число уровней квантования может быть различным. Как было показано, обычно m лежать в пределах от 1 до 15, в особо ответственных случаях параметр m может быть увеличен до 31 или 63.

С целью повышения оптимального сочетания энергетических характеристик и маскирующих свойств прицельной помехи целесообразно формировать ее таким образом, чтобы обеспечить равновероятное появление отдельных уровней.

Для получения хороших энергетических показателей прицельной помехи, рекомендуется компенсация ее постоянной составляющей.

Большое влияние на защищенность по отношению к методам компенсации помех оказывает параметр η, характеризующий степень подобия излучения разряда помехи и сигнала. Естественно, что излучатель помехи должен быть по своим электромагнитным характеристикам в максимальной степени подобен излучателю опасного сигнала. Считается хорошим результатом, обеспечивающим высокие маскирующие свойства, получения значения параметра $\eta > 0{,}8$ в одноканальной схеме.

Если за пределами контролируемой зоны в некоторых направлениях достигается меньшее значение параметра η, то могут быть рекомендованы многоканальные схемы.

Для измерения в реальных условиях параметра η в генераторе прицельной помехи должно быть предусмотрено создание специального тестового режима, когда генерируется периодическая последовательность импульсов помехи, эквивалентных по излучению одному разряду опасного сигнала.

Таким образом САЗ ПП реализованные в соответствии с схемой (рис. 5) могут использоваться для активной маскировки всех основных типов опасных сигналов, характерных для современных корпоративных сетей, с учетом ограничения по тактовой частоте, накладываемых формулой (2).

По своим техническим характеристикам системы активной защиты могут быть использованы для защиты практически любых технических средств корпоративных сетей.

Однако сложность САЗ возрастает пропорционально количеству опасных сигналов, подлежащих маскировке, и количеству узлов и блоков, имеющих высокие уровни побочных излучений.

Преимуществом методов активной защиты по сравнению с методами пассивной защиты является то, что для каждого технического средства корпоративной сети, требуемый уровень защиты может обеспечиваться индивидуально. При общем же экранировании существует проблема сочетания в одном комплексе устройств с разными уровнями защиты.

Список литературы

1. *Защита* от радиопомех/Под ред. М.В. Максимова.- М.: Сов.радио, 1967. -496 с.

2. *Нормы* эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН. -М.: МОП, 1977. -35 с.

3. *Специальные* требования по защите объектов ЭВТ второй категории от утечки информации за счет ПЭМИН. – М.: Гостехкомиссия СССР, 1979. - 44 с.

4. *Специальные* требования по защите объектов ЭВТ третьей категории от утечки информации за счет ПЭМИН. – М.: Гостехкомиссия СССР, 1979. - 43 с.

5. *Хмелевский И.В.* Анализ эффективности использования аддитивных помех для маскировки передачи речи методом дельта-модуляции.- Диссертация кандидата технических наук. Свердловск. -1989. -182 с.

6. *Гуткин Л.С.* Теория оптимальных методов радиоприема при флюктуационных помехах: 2-е изд.- М.: Сов радио,1972. -448 с.

7. *Левин Б.Р.* Теоретические основы статистической радиотехники: в 3-х томах, т.2.- М.: Сов.радио, 1975.-552 с.

8. *Новиков А.А.* Нормированные величины сигнал-помеха для сигналов с частотной и фазовой модуляцией, применяемых в системах телеобработки информации // Вопросы специальной радиоэлектроники. Серия "Электронная вычислительная техника", 1982, вып.3,- с.84-88.

9. *Вакман Д.Е.* Асимптотические методы в линейной радиотехнике. -М.: Сов.Радио, 1962.-373 с.

10. *Вайнштейн Т.Г.* Теория обработки сигналов автоматического управления в радиоэлектронных системах.- Л.: МО, 1992.-245 с.

11. *Втаонкин В.М., Каркаускас Ш.М.* Генератор импульсного случайного потока //Труды Рязанского политехнического института, вып.64.Рязань, 1975. - с.17-25.

12. *Левин Б.Р.* Теоретические основы статистической радиотехники: в 3-х томах, т.1.- М.: Сов. Радио, 1974.-392 с.

13. *Тихонов В.И.* Выбросы случайных процессов.-М.: Наука, 1970.- 375 с.

14. *Шеннон К.Э.* Работы по теории информации и кибернетике /Пер. с англ. -М.: Иностранная литература, 1963.-829 с.

15. *Положення* про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99. № 1229.

Поступила 29.08.2006