УДК 004.056

А.А. Петров,
А.А. Мельникова

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Даны рекомендации по построению систем активной защиты (САЗ) в сетях общего пользования (СОП) с применением прицельной помехи (ПП).
Ключевые слова: *системы активной защиты информации, сеть общего пользования, прицельная помеха.*

Надано рекомендації щодо побудови систем активного захисту у мережах загального користування (МЗК) з використанням прицільної завади (ПЗ).
Ключові слова: *системи активного захисту інформації, мережа загального користування, прицільна завада.*

Recommendations about the construction of active security systems in the networks of general usage with a spot jamming application are suggested.
Keywords: *systems of an information active security, network of general usage, spot jamming.*

Представим общую структурную схему САЗ ПП (рис. 1), предназначенную для маскировки побочных электромагнитных излучений одного опасного сигнала. Датчик случайного двоичного числа (ДСДЧ) синхронизируется тактовым генератором (ТГ), который синхронизирован с опасным сигналом [1, 2]. 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.

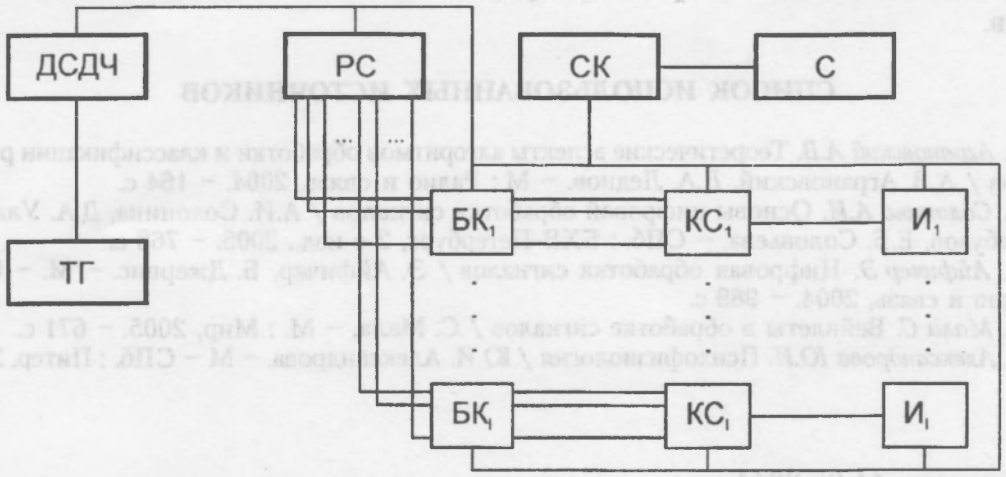

Рис. 1. Структурная схема одноканальной САЗ ПП

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, $F_в$.

Получим оценку для верхней частоты спектра аналогового шума :

$$F_в > 2 \cdot \sqrt{3} \cdot m \cdot F_т \qquad (1),$$

где $F_т$ – тактовая частота опасного сигнала.

Для помехи с параметром $m=15$ верхняя частота спектра аналогового шума, используемого при его формировании 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 лежат 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, получение значения параметра $\eta>8$ 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.

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

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 СОП, требуемый уровень защиты может обеспечиваться индивидуально. При общем же экранировании существует проблема сочетания в одном комплексе устройств с разными уровнями защиты.

Применение систем активной защиты, использующих прицельные помехи, обеспечивает эффективную защиту кабельных линий в корпоративных сетях и внутренних интерфейсов рабочих станций и серверов. В этом случае возможно получение маскирующей способности и защищенности по отношению к методам селекции и компенсации близким к предельным за счет того, что легко обеспечивается электромагнитное подобие излучателей опасного сигнала и прицельной помехи. При защите кабельных линий связи положительный эффект может быть достигнут за счет сочетания так называемого "кодового зашумления", приводящего к увеличению вероятности ошибочного декодирования в каналах связи, с САЗ ПП. При этом наличие дополнительных помех в каналах утечки способствует тому, что "кодовое зашумление" становится более эффективным как с точки зрения получения меньшей избыточности кода, так и с точки зрения увеличения вероятности ошибки приема опасных сигналов и при перехвате ТСР побочных излучений.

Выводы. Проблема защиты некоторых электромеханических устройств в силу их конструктивных особенностей и наличия низких частот в спектре опасных сигналов, достаточно полно может быть решена только при наличии прицельных помех.

Следует особо отметить, что прицельная помеха является эффективным способом блокирования канала утечки, образованного за счет неравномерности потребления тока сети. В наибольшей степени это относится к тем устройствам, где тактовая частота выше частоты сети, что приводит к эффекту потери

информации от каждого разряда, и имеется возможность регистрировать некоторую интегральную реакцию нескольких разрядов [3, 4]. В этом случае воздействие прицельной помехи подобно воздействию идеальной помехи на сигналы параллельного кода, что дает значительный маскирующий эффект.

Цифровой способ формирования прицельной помехи может использоваться и для борьбы с накоплением информации за счет ее регулярного повторения, что особенно актуально при защите устройств отображения информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

2. *Тихонов В.И.* Выбросы случайных процессов / В.И. Тихонов. – М. : Наука, 1970. – 375 с.

3. *Белинский Б.А.* Определение характеристик направленности побочного электромагнитного излучения средств вычислительной техники / Б.А. Белинский // Материалы II Международной научно-практической конференции "Безопасность информации в компьютерных системах и связи". – К., 1996. – 42 с.

4. *Веретягин А.А.* Теория обработки сигналов автоматического управления в радиоэлектронных системах / А.А. Веретягин. – Л. : МО, 1992. – 245 с.

Отримано 04.05.2011