Для оценки информационных показателей, определяющих защищенность цифровых и аналоговых речевых сигналов по единому критерию, получены выражения, которые позволяют реализовать СИА.

Литература

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. – СПб.: ГУАП, 2006. –188 с.

2. Алексеев, А.А., Кириллов, А.Б. Технический анализ сигналов и распознавание радиоизлучений. – СПб.: ВАС, 1998.–368 с.

3. Дворников, С.В. Теоретические основы синтеза билинейных распределений. – СПб.: Изд-во Политехн. ун-та, 2007. 268 с.

4. Зюко, А.Г., Финк, Л.М., Кловский Д.Д. Теория передачи сигналов. // Под ред. М.В., Назарова. – М.: Связь. 1980.

5. Зюко, А.Г. и др. Помехоустойчивость и эффективность систем передачи информации. – М.: Радио и связь. – 1985.

В.К.ЖЕЛЕЗНЯК, К.Я.РАХАНОВ, Д.С.РЯБЕНКО
В.В.БУСЛЮК, С.И.ВОРОНЧУК, И.В.ЛЕШКЕВИЧ
С.С.ДЕРЕЧЕННИК

МЕТОДИКА ОЦЕНКИ ДЛЯ ОПЕРАТИВНОГО КОНТРОЛЯ ИСТОЧНИКОВ ШУМОВОГО СИГНАЛА

Эффективность любой информационной системы оценивают интегральным и частными показателями, одним из которых является степень защиты информации (ЗИ) информационной системы.

Степень защиты информации определяют её мерой, которая устанавливает полноту выделения и оценки существенных факторов, формирующих технические требования к параметрам ЗИ. Мера ЗИ зависит от рационального использования ресурсов, выделенных на ЗИ. Требования к ЗИ определяются функциональным назначением, структурой и параметрами информационной системы. Методы и средства ЗИ формируют с учетом особенностей эксплуатации объекта информатизации, ценности информации, выделяемых сигналов (видео-, речевой, передача данных, простые, сложные), обрабатываемых на объекте.

Разрушение каналов утечки информации (КУИ) со скрытым функционированием информационной системы обеспечивают схемно-конструктивными решениями и средствами ЗИ. Схемно-конструктивные решения реализуют взаимную компенсацию информационных полей рассеивания, срыв паразитных генераций, ослабление информационных мультипликативных ВЧ-излучений, их локализацией и рассогласованием среды распространения.

Важным является разрушение КУИ активными способами – путем маскирования информационных и демаскирующих параметров сигналов маскирующими помехами. Активные методы ЗИ основаны на формировании преднамеренных шумов, обладающих необходимой эффективностью по заданному критерию эффективности, выбор которого обоснован в [1].

Маскирующие помехи, сформированные непосредственно из сигнала (видео-, речевой), наиболее адаптированы к его параметрам [2]. В качестве источников генерации преднамеренных маскирующих шумов широко распространены шумовые диоды.

Основные параметры и характеристики помехи определяются источниками генерации преднамеренных маскирующих шумов, а усилительные каскады формируют частотный диапазон, при необходимости ограничивая его. Необходимые коррекции вводятся для регулировки напряжения, мощности выходных сигналов, согласования с нагрузкой, выполнения измерительных и контролирующих функций параметров и характеристик.

Целью исследования является оценка основных параметров диодов-генераторов шума серии ND 100, а также возможность использования их в качестве источника сигнала для генераторов маскирующего шума речевого и видеоканалов, линий передачи данных.

Технические характеристики диодов-генераторов шума представлены в таблице 1.

Таблица 1 – Технические характеристики диодов серии ND 100

Тип	Постоянное напряжение $U_{ш}$, при токе 100 мкА	Спектральная плотность напряжения шума S_U, мкВ / $\sqrt{Гц}$	Граничная частота $F_{гр}$, МГц при токе 50 мкА, не менее	Неравномерность спектральной плотности напряжения шума, δS_U, дБ при токе 50мкА, не более
ND-101L	7.0 – 11.0	70	0.1	4.0
ND-102L	7.0 – 11.0	50	0.5	4.0
ND-103L	6.0 – 9.0	30	1.0	3.0
ND-104L	6.0 – 9.0	3.0	3.0	3.0

Оценка основных параметров указанных источников шума выполнялась по приведенной ниже методике. С помощью измерительного АЦП производится преобразование аналогового шумового сигнала в дискретную форму для записи его на ПЭВМ с целью последующей оценки параметров. Время выборки при этом составляет не менее 5 секунд, частота дискретизации – не менее 400 кГц, что позволяет анализировать сигналы с частотой до 200 кГц. С целью устранения искажений, установлен фильтр нижних частот, через который пропускается входной аналоговый сигнал. Частота среза такого фильтра равна половине частоты дискретизации. Дискретные отсчеты сигнала записываются в 24-разрядном двоичном коде, представляющего цифровую форму исходного сигнала в ограниченной полосе. Фрагмент такого шумового сигнала представлен на рисунке 1.

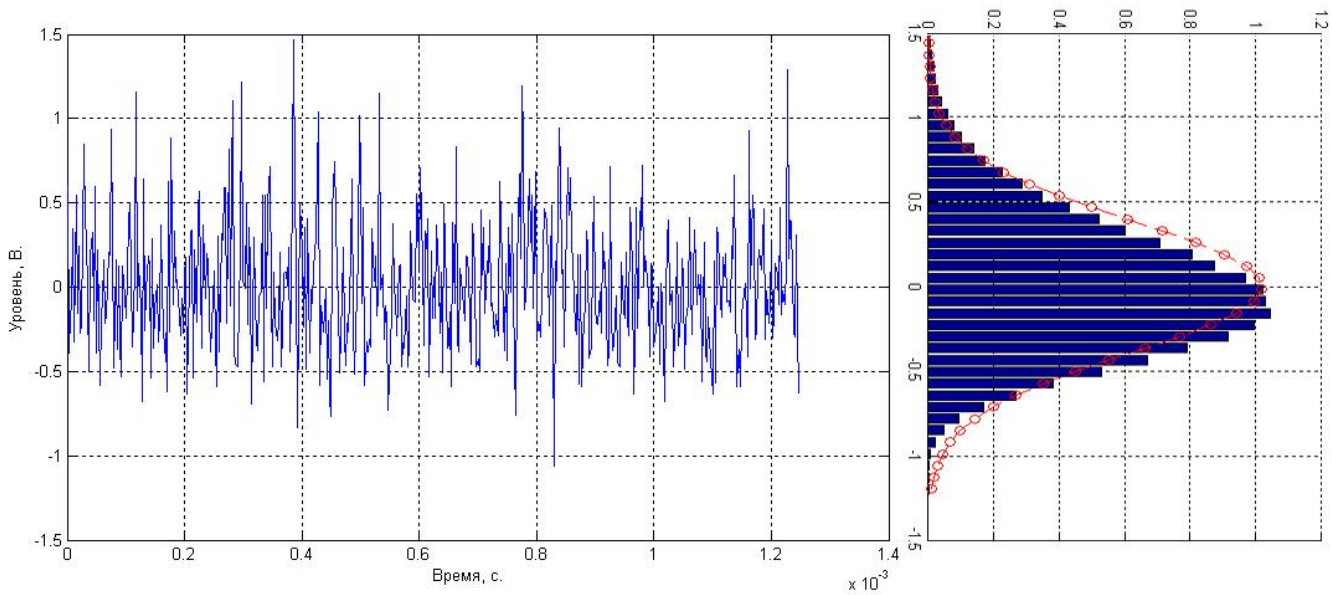

Рис. 1. Фрагмент шумового сигнала и плотность распределения его вероятности

Обобщенные характеристики шумового сигнала получены инструментально-расчетными методами. Высокая точность полученных исходных данных для расчета параметров гарантируются использованием измерительного АЦП, метрологические параметры которого аттестованы. Необходимые данные шумовых сигналов получены с помощью пакета прикладных программ MATLAB.

Обработка данных выполнена в соответствии с [3]. Оцениваемыми параметрами являлись:

– энтропийный коэффициент качества шумового сигнала (не менее 0,95);

– автокорреляционная функция (обобщенная характеристика представлена на рисунке 2);

– среднеквадратическая частота шумового сигнала (автокорреляционная функция и среднеквадратичная частота характеризуют отсутствие гармонических составляющих в спектре);

– распределение плотности вероятности шума подчинено закону Гаусса (показано с использованием критерия согласия χ^2 при уровне значимости 0,05);

– пик-фактор шумового сигнала (вверх, вниз – не менее 3);

– спектральная плотность мощности шумового сигнала равномерна в заявленных диапазонах частот.

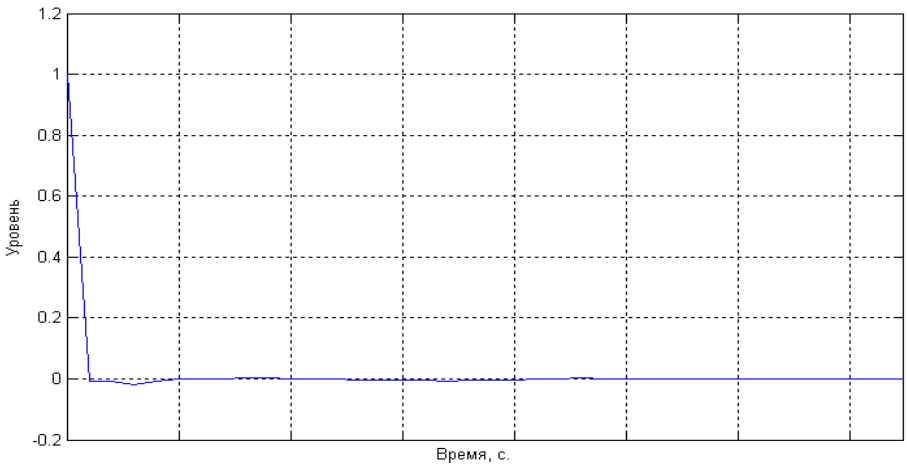

Рис. 2. Обобщенная автокорреляционная функция сигналов шумовых диодов

Выводы

В результате исследования установлены:

– высокая устойчивость метрологических параметров и характеристик (воспроизводимость результатов);

– контролепригодность параметров;

– исследованные диоды-генераторы шума превосходят известные ранее по ряду параметров (уровень излучения, неравномерность АЧХ в рабочем диапазоне частот, разброс характеристик при воздействующих факторах);

– энтропийный коэффициент качества шума, как основной параметр, приближается к единице.

На основании полученных данных достоверно показано, что диоды-генераторы шума серии ND 100 в полной мере применимы в качестве источников шумовых сигналов в генераторах маскирующего шума. Образцы таких диодов апробированы в некоторых генераторах маскирующего шума и обеспечили высокие характеристики последних.

Литература

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. ГУАП. – СПб., 2006. –188 с.

2. Железняк, В.К., Карасев, Р.С. Автоматизированная оценка маскирующего шума в речевом диапазоне частот. // Информационные системы и технологии (IST 2009): материалы V Международной конференции-форума (Минск, 16-17 ноября 2009 г.). – В 2-х ч. – Ч2. / редкол.: Н.И. Листопад [и др.]. – Минск: А.Н. Вараксин, 2009. – С.42–46.

3. Кузнецов, В.А., Ялунина, Г.В. Общая метрология. – М.: ИПК Издательство стандартов. 2001. – 272 с.

4. Буслюк, В.В., Ворончук, С.И., Лешкевич, И.В., Дереченник, С.С. Кремниевые диоды-генераторы шума серии ND 100 для криптографических систем // Комплексная защита информации: материалы XIV Межд. конференции. – Минск, 2009. – С. 61–63.

В.А.КАРАСЬ

СПОСОБЫ ЗАЩИТЫ USB ФЛЭШ-НАКОПИТЕЛЕЙ ОТ УТЕЧКИ ИНФОРМАЦИИ

Применение внешних носителей информации, в частности, USB флеш-накопителей (далее – флеш-накопитель), приводит к проблеме защиты информации. Флеш-накопители являются одним из каналов утечки информации. Большинство пользователей, использующие флеш-накопители, хранят на них не только информацию личного пользования, но и информацию ограниченного использования. Утечка или уничтожение данных, хранящихся на флеш-накопителе, может привести к нанесению ущерба.

При использовании флеш-накопителя происходит его подключение к разным ПЭВМ, что представляет дополнительную угрозу распространения шпионского программного обеспечения и вредоносного программного кода. Данная канал распространения вредоносного программного кода является самым значимым.

Средств противодействия угрозам при использовании флеш-накопителей известно много, однако наиболее адекватную и надежную защиту в состоянии обеспечить только система контроля использования внешних устройств, в числе функций которой обязательно должны присутствовать: ведение журнала аудита событий безопасности; мониторинг действий пользователей; "теневое" копирование; шифрование данных, передаваемых на USB флеш-накопитель. Однако есть и другой выход – использование специализированных USB флеш-накопителей информации.

В докладе рассматриваются каналы утечки информации с USB флеш-накопителей и способы их защиты, методы и средства предотвращения утечек информации с USB флеш-накопителей, приводятся рекомендации по использованию специализированных USB накопителей на объектах информатизации разных категорий.

А.И.КОХАН

СОВРЕМЕННЫЕ МЕТОДЫ ВЕРИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Надежность и безопасность – наиболее важные требования к программному обеспечению (ПО) в случаях его применения на наиболее важных стратегических объектах: