2. Common Evaluation Methodology for Information Technology Security. Version 0.6 11.01.97

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ХАОС-ПРЕОБРАЗОВАНИЙ

В.А. ЧЕРДЫНЦЕВ, А.Н. МОЛОСНОВ

Преобразование сообщений на основе нелинейных динамических систем (НДС) обеспечивает относительно высокую степень защиты информации в каналах связи. Рассматривается класс преобразований, использующих нелинейные дифференциальные уравнения и нелинейные отображения. Формулируются условия неискажённого воспроизведения сообщений, оценивается влияние мультипликативных и аддитивных помех на качество обобщённой синхронизации систем.

Даётся классификация методов модуляции хаос-процессов, порождаемых НДС: линейные и нелинейные. Линейные методы основаны на отображениях вида:

$$x_{n+1} = \lambda_n + F(x_n,...,x_{n-k}),$$

где λ_n – сообщение, x_n – преобразованное сообщение, $F(...)$ — нелинейная функция.

Нелинейные методы предполагают модуляцию параметров и начальных условий в отображении:

$$x_{n+1} = F(x_n,...,x_{n-k},\lambda_n)$$

Обсуждаются вопросы синхронизации прямых и обратных преобразователей в присутствии аддитивных и мультипликативных канальных помех. Формулируются условия обеспечения качественной синхронизации и выделения сообщений. Приводятся примеры построения систем передачи данных с хаос-процессами.

Показано, что простейшие НДС (1, 2-го порядков) обеспечивают эффективное хаотическое кодирование и декодирование данных. Приводятся результаты моделирования хаос-преобразователей.

Приводятся примеры построения псевдохаотических генераторов для криптографии, стойкость которых обеспечивается чувствительностью к начальным условиям и вычислительной непредсказуемостью одномерных отображений.

ПРЕОБРАЗОВАНИЕ ДИСКРЕТНЫХ СООБЩЕНИЙ В КАНАЛАХ С ЗАЩИТОЙ ИНФОРМАЦИИ

А.Н. МОЛОСНОВ, Ю.А. ТИХАНОВИЧ, П.В. ЛУЧЕНОК

Рассмотрены системы, описываемые нелинейными отображениями фрактального типа, обеспечивающие прямое и обратное преобразование сообщений в каналах с защитой информации:

$$x_{n+1} = k_1 F(x_n) + y_n$$

$$x_n = k_2 F(x_{n-1})$$

где x_n – преобразованное сообщение, $F(...)$ – нелинейная функция, y_n – сообщение.

Возможны два режима работы системы: генерация хаотических колебаний и нелинейное преобразование сообщения.

Выявлены условия, при которых возникает режим хаотических движений в системе. Показана возможность восстановления сообщений в случае действия аддитивных помех в канале передачи.

Обсуждаются вопросы синхронизации генераторов хаотических колебаний на передающей и приёмной сторонах, влияние канальных помех на качество синхронизации.

За счёт включения линейного фильтра с оптимальными характеристиками на выходе обратного преобразователя снижается вероятность ошибочного воспроизведения информационных символов y_n.

Приведены результаты моделирования системы. Приводятся трёхмерные отображения состояний системы при различных параметрах преобразований.

Показана возможность повышения качества криптозащиты информации за счёт использования комбинационного построения генераторов хаотических последовательностей.

ШИРОКОПОЛОСНАЯ СИСТЕМА СВЯЗИ С ЗАЩИТОЙ ИНФОРМАЦИИ

Д.А. ГОЛОВАЧ, Н.А. ДЕЕВ

Рассмотрена система передачи сообщений, использующая скремблированный ЧМ-сигнал $s(t)$ в качестве скремблирующих последовательностей, обеспечивающих расширение спектра ЧМ-сигнала, используется двоичная $\{\pm 1\}$ случайная последовательность (ДСП) $g(t)$ с тактовой частотой $f(t)$. Последовательностью $g(t)$ осуществляется фазовая манипуляция ЧМ-сигнала. Для обеспечения

энергетической скрытности системы ДСП $g(t)$ формируется как произведение двух двоичных последовательностей: псевдослучайной (ПСП) $g_1(t)$ и случайной $x(t)$, представляющей клиппированный физический шум; полоса спектра которого меньше полосы спектра ПСП $g_1(t)$:

$$s(t) = g_1(t)x(t)\cos[\omega_0 t + \psi(t,\lambda)]$$

Обработка фазоманипулированного сигнала сводится к операции дескремблирования в корреляторе с опорной ПСП $g_1(t)$, фильтрации в полосовом фильтре полученного сигнала $x(t)\cos[\omega_0 t + \psi(t,\lambda)]$, операции свёртки для получения ЧМ-сигнала и, наконец, выделению сообщения в частотном детекторе.

Обсуждаются вопросы помехоустойчивости системы при действии флуктуационных и полосовых помех.

Сравниваются два варианта свёртки сигнала: путём возведения в квадрат, и с помощью схемы с обратной связью по дискретному процессу $x(t)$. Доказывается, что второй вариант обеспечивает более высокое качество воспроизведения сообщения.

ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ, ВЫПОЛНЕННЫЕ МЕТОДОМ ВАКУУМНОГО НАПЫЛЕНИЯ

Е.А. УКРАИНЕЦ, Т.В. БОРБОТЬКО, А.В. ГУСИНСКИЙ, И.А. ВРУБЛЕВСКИЙ

Постоянное совершенствование специальной техники стимулирует появление новых, все более эффективных электромагнитных экранов, в том числе и для защиты от утечки информации по техническим каналам из специальных защищенных помещений, в частности, помещений для обработки шифрованной информации, комнат для ведения конфиденциальных переговоров, камер для настройки и испытаний специальной техники и т.д. А так же используемых для экранирования средств обработки информации для локализации ПЭМИН.

Для создания гибких конструкций электромагнитных экранов весьма перспективной является возможность применения технологии вакуумного напыления тонких пленок на машинно-вязаные основы.

Для изучения экранирующих свойств изготавливались образцы, на которые в натянутом состоянии методом магнетронного распыления наносилось металлическое покрытие из никеля, толщиной 0,1 нм.

После чего из этого полотна формировались конструкции с геометрическими неоднородностями. Одна из них представляла собой гребенчатую структуру с шагом гребня 1 см, вторая – имела поверхность псевдопирамидальной формы.

Экранирующие свойства материалов исследовали с помощью измерителя КСВН панорамного Р2-65, генератора РГ4-14 и индикатора Я2Р-70 в диапазоне частот 27-115 ГГц.

В результате исследований установлено, что использование машинно-вязаных полотен с геометрическими неоднородностями и напыленным никелевым покрытием позволяет уменьшить КСВН более чем в 2,5 раза в отличие от полотен с гладкой поверхностью.

Формирование геометрических неоднородностей на поверхности машинно-вязаных основ позволяет повысить их коэффициент ослабления (до 40 дБ) за счет поглощения ЭМИ в материале полотна (рис.).

Установленные особенности взаимодействия исследованных материалов с электромагнитным излучением позволяют использовать их при изготовлении гибких многослойных конструкций широкополосных экранов ЭМИ.

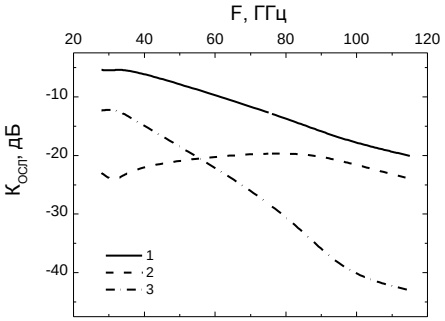

Рисунок. Зависимость коэффициента ослабления машинно-вязаных полотен с напыленным Ni от частоты: 1 — полотно гладкой формы, 2 —