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