# ПОЛУЧЕНИЕ ДЛИННЫХ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Дрыбин Е. А., Садов В. С.
Кафедра интеллектуальных систем, Факультет радиофизики и компьютерных технологий, Белорусский государственный университет
Минск, Республика Беларусь
E-mail: {ydrybin, vasiliy.sadov}@gmail.com

*В работе разработан метод получения воспроизводимых случайных последовательностей произвольной длины. Подобные последовательности востребованы в задачах современных криптографии и стеганографии. Метод основан на явлении детерминированного хаоса.*

## Введение

Получение случайных последовательностей чисел является краеугольным камнем многих прикладных задач современных крипто- и стеганографических систем защиты информации (генерация ключей, контейнеров, одноразовых шифроблокнотов и т.д.). Источниками настоящих случайных чисел могут служить физические шумы, как, например, дробовой шум в резисторе, детектор событий ионизирующей радиации. Однако случайные последовательности, полученные с помошью подобных устройств невозможно воспроизвести, что делает их непригодными для решения ряда задач. В большинстве приложений информационной безопасности используются генераторы псевдослучайных чисел (ГПСЧ). Хотя псевдослучайная последовательность (ПСП), как может показаться, лишена закономерностей, любой ГПСЧ с конечным числом внутренних состояний повторится после достаточно длинной последовательности чисел. Таким образом, для большинства ГПСЧ возможно вычислить всю ПСП, если их состояние скомпрометировано, что позволит криптоаналитику получить доступ не только к будущим сообщениям, но и ко всем предыдущим. В настоящей работе решается задача получения воспроизводимых случайных последовательностей чисел на основе явления детерминированного хаоса.

## I. Явление детерминированного хаоса

Явление детерминированного хаоса – это возникновение неупорядоченных движений в совершенно детерминированных системах. Основной причиной возникновения непредсказуемости состояния нелинейной динамической системы является совокупность неустойчивости всех или почти всех состояний такой системы и задания начальных условий с конечной точностью [1]. Важными свойствами хаотических последовательностей являются:

- качественные характеристики (автокорреляция, спект мощности) идентичны характеристикам случайной последовательности;
- в отличие от случайных последовательностей их возможно воспроизвести на некотором протяжении, после чего исходная и воспроизведенная последовательности существенно расходятся.

Очевидно, что такая последовательность лишена недостатков ПСП, однако возникает два взаимосвязанных вопроса:

- какова длина хаотической последовательности, которую можно воспроизвести?
- каким образом получить сколь угодно длинную хаотическую последовательность, не изменяя ее качественные характеристики?

Исследовательсая часть настоящей работы призвана решить вышеперечисленные вопросы и разработать метод, позволяющий получать длинные случайные последовательности.

## II. Генерация длинных последовательностей

В качестве генератора хаотических последовательностей в настоящей работе использовалась известная система Лоренца (для моделирования использовался пакет программ MATLAB):

$$\dot{X} = -\sigma X + \sigma,$$

$$\dot{Y} = -XZ + \rho X - Y,$$

$$\dot{Z} = XY - \beta Z$$

(при управляющем параметре $\rho = 28$ и $\sigma = 10, \beta = 8/3$). В ходе исследования экспериментально обнаружена обратно пропорциональная зависимость длины воспроизведения последовательности от порядка величины флуктуации начальных условий от абсолютной величины [2]:

$$l = -k(R) \cdot \epsilon.$$

где $l$ – количество воспроизводимых отсчетов, $k$ – коэффициент воспроизводимости зависящий от $R$ – минимального удовлетворяющего уровня корреляционной функции, $\epsilon$ – порядок флуктуации начальных условий относительно абсолютного значения. Для определения степени воспро-

изводимости хаотического сигнала воспользуемся корреляционной функцией:

$$R(l) = \frac{\sum_{i=0}^{k}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=0}^{k}(x_i - \bar{x})^2 \sum_{i=0}^{k}(y_i - \bar{y})^2}}.$$

Будем считать сигнал воспроизводимым на $l$ отсчетах для значения $R > 0.99$. Для системы Лоренца экспериментально установлен коэффициент $k_{0.99} = 190$ [2]. В пакете программ MATLAB максимально достижимая точность чисел равна $10^{-15}$, таким образом для идентичных начальных условий $\epsilon = 16$. Максимально возможная длина воспроизводимой последовательности состfвляет около 3000 отсчетов после чего исходная и воспроизведенная последовательности начнут существенно расходиться.

Для получения воспроизводимой хаотичной последовательности длиной более 3000 отсчетов необходимо перезапускать генератор, не нарушая при этом качественных свойств последовательности. Очевидно, если криптоаналитик сумеет выявить длину и границы каждого цикла генерации, то криптографическая стойкость системы будет существенно снижена. Для сокрытия мест «сшивки» $n$-ый перезапуск генератора необходимо осуществлять с $nL + 1$-го отсчета. Таким образом, получается сколь угодно длинная непрерывная хаотическая последовательность, не отличающаяся от «цельной» последовательности такой же длины (рис. 1, 2) [2]. Для воспроизведения исходной последовательности при таком способе перезапуска генератора требуется передавать соответствующие наборы начальных условий ($nL + 1$-ые отсчеты) в кодируемом сообщении.

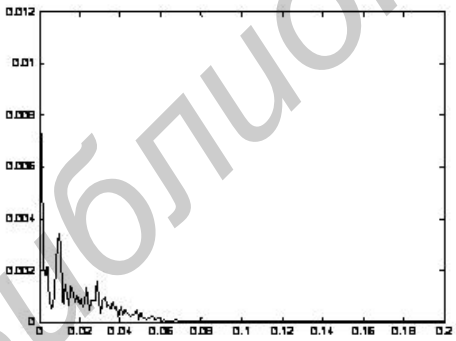

Рис. 1 – Спектр мощности «сшитой» хаотической последовательности

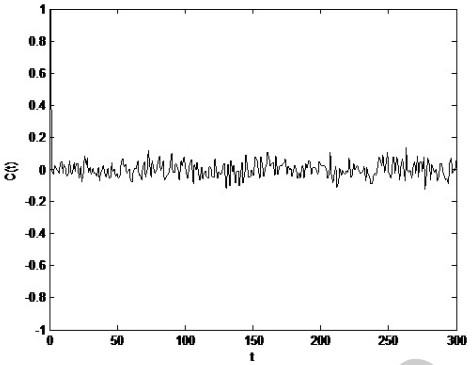


Рис. 2 – Автокорреляционная функция «сшитой» хаотической послоедовательности

## Заключение

В большинстве систем защиты информации от «качества случайности» используемых ГПСЧ напрямую зависит качество получаемых результатов. В настоящей работе рассмотрен способ получения воспроизводимых последовательностей произвольной длины на основе явления детерминированного хаоса. В отличие от ПСП подобные последовательности идентичны по характеристикам случайным, что позволяет успешно использовать их в крипто- и стегосистемах.

## Список литературы


1. Шустер, Г. Детерминированный хаос: введение / Г. Шустер // М.: Мир – 1988. – С. 240.
2. Садов, В. С., Дрыбин, Е. А. Исследование хаотических процессов на примере математической модели системы Лоренца в пакете Matlab r2011b / В. С. Садов, Е. А. Дрыбин // Информационные технологии и системы 2012 (ИТС 2012): материалы международной научной конференции.- Минск: БГУИР, 2012.-С. 270-271.