

В данной работе проводится сравнение указанных методов встраивания информации. Оказывается, что нельзя выбрать какой-то универсальный метод который бы можно было использовать во всех случаях, а необходимо оценить требования к результату и имеющиеся средства, и на основе их выбирать оптимальный для использования в конкретной ситуации метод.

Литература

1. Cox I.J., Kilian J., Leighton T., Shamoon T.G. *A secure, robust watermark for multimedia* // Information hiding: first international workshop. Lecture Notes in Comp. Science. 1996. Vol. 1174. P. 183–206.
2. Barni M., Bartolini F., Cappellini V., Lippi A., Piva A. *A DWT-based technique for spatio-frequency masking of digital signatures* // Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents. 1999. Vol. 3657.

О ВЫЯВЛЕНИИ СТОХАСТИЧЕСКИХ ЗАВИСИМОСТЕЙ СЛОЖНОЙ СТРУКТУРЫ В ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

Мальцев М.В.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь maltsew@bsu.by

Псевдослучайные последовательности (ПСП) играют важнейшую роль в системах криптографической защиты информации. Генераторы ПСП используются для получения ключей криптосистем, гаммы поточных шифров, параметров криптографических алгоритмов и протоколов. Выходные значения стойких алгоритмов шифрования и хэширования также являются ПСП. Для оценки качества ПСП сравниваются с равномерно распределенной случайной последовательностью (РПС) — математической моделью «чистой случайности». Случайная последовательность $\{x_t \in \{0, 1, \dots, N-1\} : t \in \mathbb{N}\}$ является РПС, если для нее выполняются следующие два свойства [1]:

1. Для любого $n \in \mathbb{N}$ и для любых $1 \leq t_1 < t_2 < \dots < t_n$ случайные величины $x_{t_1}, \dots, x_{t_n}$ независимы в совокупности.
2. Случайная величина x_t равномерно распределена на множестве $\{0, 1, \dots, N-1\}$ для любого $t \in \mathbb{N}$:

$$P\{x_t = j\} = \frac{1}{N}, \quad j \in \{0, 1, \dots, N-1\}.$$

Стойкие генераторы ПСП по своим свойствам должны быть неотличимы от РПС. Для обнаружения в ПСП отклонений от РПС используются наборы статистических тестов, называемые батареями. Наиболее известной и часто используемой на практике является батарея тестов NIST, разработанная лабораторией информационных технологий Национального института стандартов и технологий США [2]. Элементы РПС должны быть независимыми, однако традиционные батареи тестов не позволяют обнаруживать сложные стохастические зависимости большой глубины $s \gg 1$, поэтому для их выявления требуются дополнительные исследования. Универсальной математической моделью, описывающей такие зависимости, является цепь Маркова порядка s . К сожалению, число ее параметров увеличивается экспоненциально с ростом s , поэтому непосредственное применение этой модели на практике ограничено малыми значениями порядка. Для решения этой проблемы разрабатываются специальные малопараметрические (parsimonious) марковские модели, число независимых параметров которых зависит от s полиномиально, что позволяет строить на их основе алгоритмы статистического тестирования для обнаружения в генераторах ПСП сложных стохастических зависимостей большой глубины [3].

В работе [4] рассматривались двоичные последовательности, полученные с помощью функции `rand` стандартной библиотеки языка программирования Си. Статистическое тестирование на основе батареи NIST не выявило отклонений от РПСП, тогда как проведенные нами компьютерные эксперименты с использованием разработанных алгоритмов на основе специальных малопараметрических марковских моделей позволило обнаружить стохастические зависимости между элементами последовательности.

Литература

1. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. *Криптология*. Минск: БГУ, 2014.
2. A statistical test suite for random and pseudorandom number generators for cryptographic applications: National Institute of Standards and Technology Special Publication 800-22 Rev. 1a, 2010.
3. Мальцев М.В., Харин Ю.С. *О стохастическом моделировании криптографических генераторов на основе малопараметрических моделей* // Комплексная защита информации: материалы XXII научно-практической конференции, Полоцк, 16–19 мая 2017. С. 120–123.
4. Wang Y., Nicol T. *Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL* // Computers and Security, № 53, 2015. — P. 454–471.

МОДЕЛИ С МАРКОВСКИМИ ПЕРЕКЛЮЧЕНИЯМИ СОСТОЯНИЙ ДЛЯ АНАЛИЗА ЦИКЛОВ ЭКОНОМИЧЕСКОЙ АКТИВНОСТИ

Малюгин В.И.

Белгосуниверситет, факультет прикладной математики и информатики
Независимости 4, 220030 Минск, Беларусь Malugin@bsu.by

Модели с переключением состояний находят широкое применение для анализа процессов с циклической сменой классов состояний [1]. В докладе представляется разработанная методика построения и применения эконометрических моделей с марковскими переключениями состояний, включающими опережающий индикатор, для анализа поворотных точек и прогнозирования циклических изменений экономической активности [2–5].

Описываются построенные в соответствии с методикой модели для годовых темпов роста реального ВВП Республики Беларусь ($GGDP_t$) с опережающим индикатором в виде рассчитываемого индекса экономических настроений (ESI_t) [4] для двух классов состояний экономики: класса 0 — «замедление и спад» и класса 1 — «восстановление и рост». Установлена коинтеграционная зависимость между временными рядами $GGDP_t$ и ESI_t , которая лежит в основе построенных моделей, предназначенных для оценивания поворотных точек и прогнозирования цикла экономической активности белорусской экономики. Показано, что лучшими прогностическими способностями обладает модель MS-LR (*MS-Linear Regression*) вида:

$$GGDP_t = c_{d(t)} + \beta_{d(t),1}t + \beta_{d(t),2}ESI_t + \xi_t, \quad t = 1, \dots, T,$$

где ξ_t — стационарный процесс; $d_t \in \{0, 1\}$ ($t = 1, \dots, T$) — номера классов состояний, описываемые однородной эргодической цепью Маркова [6].

На рисунке 1 приводятся: временной ряд годовых темпов роста реального ВВП (переменная $GGDP$, черная линия), его цикл ($GGDP_sp$, светлая линия), построенный с помощью фильтра Ходрика-Прескотта, а также прогнозы для обоих классов состояний и результаты периодизации цикла на основе модели MS-LR (серые вертикальные полосы соответствуют классу 0).