УДК 681.3.06

МЕТОДИКА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

к.т.н. А.В. Потий, С.Ю. Орлова, Т.А. Гриненко
(представил д.т.н., проф. И.Д. Горбенко)

В статье рассматривается методика статистического тестирования генераторов случайных и псевдослучайных чисел, используемых в криптографических приложениях. Описываются критерии принятия решений по прохождению двоичными последовательностями статистических тестов.

Введение. Тестирование генераторов случайных и псевдослучайных чисел (ГСЧ и ГПСЧ), используемых в криптографических приложениях, является актуальной задачей как в практическом, так и в теоретическом плане. Несмотря на значительные наработки в данной области, разработчики, тем не менее, нуждаются в удобном инструментарии, способном предоставить приемлемую метрику, которая позволит достаточно ясно исследовать степень случайности последовательностей, порождаемых ГСЧ (ГПСЧ). Кроме того, необходимо обеспечить разработчиков достаточным объемом информации для принятия решения относительно «качества» генератора.

На сегодняшний день разработано достаточно большое количество различных типов ГСЧ (ГПСЧ). Однако для демонстрации их статистических свойств использовались различные подходы к статистическому тестированию. Таким образом, сложилась ситуация, которая характеризуется тем, что невозможно объективно сравнить различные генераторы с единых позиций. Выходом из этого положения является использование некоторого стандартного набора статистических тестов, объединенных единой методикой расчета необходимых показателей эффективности ГПСЧ и принятия решения о случайности формируемых последовательностей. Наиболее известным набором статистических тестов является набор из пяти тестов, предложенный Кнутом в его классической работе «Искусство программирования для ЭВМ» [1]. Решению этой задачи были посвящены ряд работ отечественных авторов [2, 3, 4]. Однако, предложенные решения обладали недостатками, которые оказали влияние на их практическую значимость. Так, в [1] были предложены только тесты, тогда как вопросы методики их применения рассматриваются недостаточно полно. В работе [3] предложена оригинальная методика применения тестов и принятия решения относительно свойств генератора, кото-

рая получила свое дальнейшее развитие в [4]. Однако, этим работам присущ один недостаток – ограниченное количество статистических тестов.

В США был сделан первый шаг к стандартизации набора статистических тестов путем принятия в 1994 году национального стандарта «Требования безопасности к криптографическим модулям» [5]. Однако, требования и методика стандарта больше носят технологический характер. Они направлены на решение задачи статистического контроля используемых в криптографических модулях псевдослучайных последовательностей и в общем случае малопригодны к решению задачи исследования статистических свойств ГПСЧ.

В 1999 году специалистами NIST, в рамках проекта AES (Advanced Encryption Standard) был разработан набор статистических тестов NIST STS (NIST Statistical Test Suite) и предложена методика проведения статистического тестирования ГСЧ (ГПСЧ) [6], которые на настоящий момент наилучшим образом отвечают потребностям всех заинтересованных сторон.

В данной работе рассматриваются критерии принятия решения о прохождения последовательностью статистического теста и методика тестирования ГСЧ (ГПСЧ).

1. ***Критерии принятия решения о прохождении теста.*** Для принятия решения о прохождении последовательностью случайных (псевдослучайных) чисел статистического теста используются следующие три основных вычислительных подхода.

Пусть дана двоичная последовательность $\mathbf{S = \{s_1, s_2, \ldots, s_n\}}$, $\mathbf{s_i \in \{0,1\}}$, длиной **n** бит. Необходимо принять решение, проходит данная последовательность статистический тест или нет. Возможны следующие подходы к решению этой задачи.

1. Критерий принятия решения на основе задания порогового уровня. Данный подход основан на вычислении по данной последовательности **S** статистики теста **c(S)** с её последующим сравнением с некоторым пороговым уровнем $\mathbf{c_{пор}(S)}$. Критерий принятия решения формулируется следующим образом: считается, что двоичная последовательность **S** не проходит статистический тест всякий раз, когда статистика теста **c(S)** принимает значение меньшее, чем пороговый уровень $\mathbf{c_{пор}(S)}$.

2. Критерий принятия решения на основе задания фиксированного доверительного интервала. При данном подходе критерий принятия решения формулируется следующим образом: считается, что двоичная последовательность **S** не проходит статистический тест, если значение статистики теста **c(S)** находится вне пределов доверительного интервала значений статистики, вычисленного для заданного уровня значимости α.

Данный критерий является более надежным по сравнению с первым. Необходимо только учитывать, что различным уровням значимости будут соответствовать различные доверительные интервалы.

3. Третий подход построения критерия принятия решения опирается на вычисление для статистики теста **c(S)** соответствующего значения вероятности **P**. Здесь статистика теста рассматривается как реализация случайной величины, которая подчиняется известному закону распределения. Малые значения вероятности **P** (**P** < 0,05 или **P** < 0,01) интерпретируются как доказательство того, что последовательность не случайна. Решающее правило формулируется так: для фиксированного уровня значимости α двоичная последовательность **S** не проходит статистический тест, если значение вероятности **P** < α. Значения α рекомендуется выбирать из интервала [0,001; 0,01].

Использование данного подхода имеет дополнительное преимущество по сравнению с предыдущим, которое заключается в том, что однажды рассчитанное значение вероятности **P** может сравниваться с произвольно выбранным уровнем значимости α без проведения дополнительных расчетов.

В основу наиболее мощных библиотек статистического тестирования ГПСЧ, к которым можно отнести пакет DIEHARD [8], Crypt-SX [7] и пакет NIST STS [6], заложен именно третий критерий принятия решения.

2. ***Методика тестирования генератора.*** Любой пакет статистических тестов может использоваться для решения следующих задач:

– идентификация ГСЧ (ГПСЧ), которые формируют «плохие» двоичные последовательности;

– разработка новых ГСЧ (ГПСЧ);

– проверка корректности реализации ГСЧ (ГПСЧ);

– изучение генераторов, описанных в стандартах;

– исследование степени случайности реально используемых ГСЧ (ГПСЧ).

Основным принципом тестирования двоичной последовательности является проверка нулевой гипотезы $\mathbf{H_0}$, заключающейся в том, что тестируемая последовательность является случайной. Альтернативной гипотезой $\mathbf{H_a}$ является гипотеза о том, что тестируемая последовательность не случайна. По результатам применения каждого теста нулевая гипотеза либо принимается, либо отвергается. Решение о том, что будет ли заданная последовательность нулей и единиц случайной или нет принимается по совокупности результатов всех тестов.

Порядок тестирования отдельной двоичной последовательности **S** выглядит следующим образом.

1. Выдвигается нулевая гипотеза $\mathbf{H_0}$ – предположение о том, что данная двоичная последовательность **S** случайна.

2. По последовательности **S** вычисляется статистика теста **c(S)**.

3. С использованием специальной функции и статистики теста вычисляется значение вероятности **P** = **f(c(S))**, **P** $\in$ [0, 1].

4. Значение вероятности **P** сравнивается с уровнем значимости α,

$\alpha \in [0{,}001;\ 0{,}01]$. Если $\mathbf{P} \geq \alpha$, то гипотеза $\mathbf{H_0}$ принимается. В противном случае принимается альтернативная гипотеза.

Для принятия решения относительно генератора в целом применяют следующую методику тестирования генератора.

1. Из множества аппаратных или программных генераторов выбирают генератор **G**, который необходимо оценить и принять решение о том, что он формирует случайные двоичные последовательности. Генератор должен порождать двоичную последовательность $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $s_i \in \{0,1\}$ произвольной длины **n**.

2. Для фиксированного значения **n** формируют множество из **m** двоичных последовательностей:

$$\begin{gathered} S_1 = \{s_1, s_2, \ldots, s_n\}; \\ S_2 = \{s_1, s_2, \ldots, s_n\}; \\ \ldots\ldots\ldots\ldots\ldots \\ S_m = \{s_1, s_2, \ldots, s_n\}. \end{gathered}$$

Таким образом, для тестирования необходимо сформировать выборку объемом $\mathbf{N} = \mathbf{m} \times \mathbf{n}$.

3. Каждую последовательность подвергают тестированию с использованием пакета NIST STS. В результате формируется статистический портрет генератора следующего вида:

№ теста **j** / № пос-ти **i**	1	2	…	q
S_1	$P_{1,1}$	$P_{1,2}$		$P_{1,q}$
S_2	$P_{2,1}$	$P_{2,2}$		$P_{2,q}$
⋮	⋮			
S_m	$P_{m,1}$	$P_{m,2}$		$P_{m,q}$

$$\Rightarrow \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1q} \\ P_{21} & P_{22} & \cdots & P_{1q} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mq} \end{pmatrix}.$$

Введем понятие статистического портрета генератора. Статистический портрет генератора представляет собой матрицу размерностью $\mathbf{m \times q}$, где **m** – количество тестируемых двоичных последовательностей, а **q** – количество статистических тестов, используемых для тестирования каждой последовательности. Элементы матрицы

$$P_{ij} \in [0,1], \text{ где } i = \overline{1,m}, \quad j = \overline{1,q}$$

представляют собой значения вероятности, полученной в результате тестирования **i** - й последовательности **j** - м тестом.

4. По полученному статистическому портрету определяют долю последовательностей, прошедших каждый статистический тест. Для этого задают уровень значимости $\alpha \in [0{,}001;\ 0{,}01]$ и осуществляют подсчет

значений вероятности **P**, превышающих заданный уровень α для каждого из **q** тестов, т.е. определяют коэффициент

$$r_j = \frac{\#\left\{P_{ij} \geq \alpha \middle| i = 1,2,\ldots,m\right\}}{m}.$$

В результате формируется вектор коэффициентов $\mathbf{R} = \{r_1, r_2, \ldots, r_q\}$, элементы которого характеризуют, в процентном соотношении, прохождение последовательности S_i всех статистических тестов.

Правило 1. Считается, что генератор **G** прошел тестирование по **j** - му тесту, если значение коэффициента r_j находится внутри доверительного интервала $[r_{min}, r_{max}]$. Границы доверительного интервала определяются согласно выражению

$$r_{max(min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}},$$

где $\hat{p} = 1 - \alpha$.

5. Осуществляется статистический анализ статистического портрета. Полученные значения вероятностей P_{ij} должны подчиняться равномерному закону распределения на интервале [0, 1] [2]. Для каждого вектора-столбца статистического портрета строится гистограмма частостей F_k попаданий значений P_{ij} в каждый из **k** = 1, 2, …, 10 подинтервалов, на которые разбивается интервал [0, 1]. Равномерность распределения значений вероятностей P_{ij} проверяется с использованием критерия χ^2. Для этого вычисляется статистика вида

$$\chi_j^2 = \sum_{k=1}^{10} \frac{\left(F_k - m/10\right)^2}{m/10},$$

которая подчиняется распределению χ^2 с девятью степенями свободы.

Правило 2. Считается, что генератор **G** прошел тестирование по **j**-му тесту, если выполняется условие $\chi_j^2 > 0{,}0001$.

6. Наконец, принимают окончательное решение по генератору по следующему решающему правилу: считается, что генератор **G** прошел статистическое тестирование пакетом NIST STS, если значения коэффициентов r_j для всех $j = \overline{1,q}$ находятся внутри доверительного интервала $[r_{min}, r_{max}]$ и соблюдается условие $\chi_j^2 > 0{,}0001$ для всех $j = \overline{1,q}$.

Заключение. Рассмотренная методика тестирования и полученные с ее использованием результаты могут рассматриваться как первичный анализ генератора. На основе пакета NIST STS могут быть построены методики более глубокого статистического и структурного анализа последовательностей. Так, для более надежной оценки генераторов целесообразно проводить не одно испытание, а как минимум три (одно испытание – построение одного полного статистического портрета). При повторении выводов по генератору на основе анализа каждого из трех статистических портретов степень неопределенности относительно свойств генератора существенно уменьшится и надежность решения увеличится.

В настоящее время нами закончена разработка программного обеспечения, позволяющая применить рассмотренную методику к результатам, полученным с использованием пакета DIEHARD. Создана реальная возможность совместного использования двух мощных инструментальных средств и создания базы данных результатов тестирования генераторов псевдослучайных чисел.

ЛИТЕРАТУРА

1. Кнут Д. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т.2. – М.: Мир, 1977. – 700 с.
2. Бусленко Н.П., Голенко Д.И., Соболь И.М. и др. Метод статистических испытаний (Метод Монте-Карло). – М.: Физматгиз, 1962. – 337 с.
3. Левитан Ю.Л., Соболь И.М. О датчике псевдослучайных чисел для персонального компьютера // Математическое моделирование – 1990. – Т.2. – №8. – С.119 - 126.
4. Потий А.В., Пестерев А.К. Принципы системного подхода к сертификации генераторов псевдослучайных чисел в системах защиты информации // Радиотехника. Всеукраинский межведомственный научно - техн. сб. – 1997. – Вып.104. – С. 163 - 172.
5. Security requirements for Cryptographic Modules. FIPS 140-1. – U.S. Department of Commerse. 1994. – 54 p.
6. J.Soto Randomness Testing of the Advanced Encryption Candidate Algorithms. – NIST, 1999. – 37 p.
7. Helen Gustafson, et. al. Statistical test suite **Crypt-SX. –** Available on *http://www.isrc.qut.edu.au/cryptx*.
8. G. Marsaglia. DIEHARD Statistical Tests. – Available on *http://stat.fsu.edu/~geo/diehard.html*.

Поступила в редколлегию 26.03.2001