Standard. – Federal Register. Vol. 62, № 1. 1997. Pp. 93-94. 2. Announcing Reguest for Candidate Algorithm Nomination for Advanced Encryption Standard (AES). - Federal Register. Vol. 62, № 177. 1997. Pp. 48051-48058. 3. М. Ф. Бондаренко, И. Д. Горбенко, А. В. Потий. Улучшенный стандарт симметричного шифрования XXI века: концепция создания и свойства кандидатов. Радиотехника. Вып. 114. 2000. С. 5-15. 4. Status report on the 2-nd round of the Development of the Advanced Encryption Standard / AES home page. http://www.nist.gov/aes. 5. Status report on the 3-th round of the Development of the Advanced Encryption Standard / AES home page. http://www.nist.gov/aes. 6. Joan Daemen, Vincent Rijmen. The Rijndael Block Cipher. AES Proposal: Rijndael, Document version 2, 3. 09. 99.

УДК 681.3.06

СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ С ИСПОЛЬЗОВАНИЕМ НАБОРА СТАТИСТИЧЕСКИХ ТЕСТОВ NIST STS

Александр Потий, Светлана Орлова, Татьяна Гриненко
Харьковский государственный технический университет радиоэлектроники

Аннотация: **Рассматриваются некоторые аспекты выбора и исследования генераторов случайных и псевдослучайных чисел. Выходные данные таких генераторов могут использоваться во многих криптографических приложениях, например при генерации ключевых данных. Генераторы, которые используются в криптографических приложениях, должны удовлетворять более жёстким требованиям, чем остальные генераторы. Выходные последовательности таких генераторов должны быть непредсказуемыми. В этой статье обсуждаются критерии оценки качества и выбора надежных генераторов. Также рассматриваются статистические тесты, которые могут быть использованы как первый шаг при определении, является ли генератор пригодным для конкретных криптографических приложений. Рассматривается методика статистического тестирования генераторов.**

Summary: **This article discusses some aspects of selecting and testing random and pseudorandom number generators. The outputs of such generators may be used in many cryptographic applications, such as the generation of key material. Generators suitable for use in cryptographic applications may need to meet stronger requirements than for other applications. In particular, their outputs must be unpredictable in the absence of knowledge of the inputs. Some criteria for characterising and selecting appropriate generators are discussed in this article. The subject of statistical testing and its relation to cryptanalysis is also discussed, and some recommended statistical tests are provided. These tests may be useful as a first step in determining whether or not a generator is suitable for a particular cryptographic application.**

Ключевые слова: **Генератор случайных чисел, критерий для проверки гипотезы, *P*-значение, криптографические приложения.**

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), и 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. Чаще всего набор и методику тестирования предлагал сам разработчик генератора. 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

 ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

недостатками, которые оказали влияние на их практическую значимость. Так в [1] были предложены только тесты, тогда как вопросы методики их применения рассмотрены не достаточно полно. В работе [3] предложена оригинальная методика применения тестов и принятия решения относительно свойств генератора, которая 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 носят больше 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, набор статистических тестов NIST и приводятся результаты экспериментальных исследований свойств ряда ГПСЧ.

I 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 $S = \{s_1, s_2, \ldots, s_n\}$, $s_i \in \{0,1\}$ 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 $c_{\text{пор}}(S)$. 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* $c_{\text{пор}}(S)$.

Например, при проверке сложности последовательности с использованием теста на основе алгоритма Лемпеля-Зива, по заданной двоичной последовательности S вычисляется её статистика $c(S)$. Для того, чтобы определить, прошла ли эта последовательность тест или нет, необходимо сравнить полученное значение $c(S)$ с пороговым значением $n/\log_2 n$ [7]. Однако такой подход не является достаточно надежным. Как показали практические исследования [8] использование такого критерия часто приводит к ошибочным решениям.

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. Например, пусть к двоичной последовательности S длиной $n = 800$ бит применяется частотный тест. Значение статистики теста $c(S)$ есть число единиц в последовательности S, причём ожидается, что в последовательности будет приблизительно 400 единиц и 400 нулей. Если зафиксировать уровень значимости на уровне 5% ($\alpha = 0{,}05$), то последовательность S не пройдет частотный тест, если число единиц будет находиться вне доверительного интервала $400 \pm 1{,}96/2 \times \sqrt{800} = [373,\ 427]$.

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. Статистка теста строится таким образом, чтобы её большие значения указывали на какой-либо дефект случайности последовательности. Значение вероятности P есть вероятность того, что статистика теста примет значение большее, чем наблюдаемое на опыте в предположении случайности последовательности. Следовательно малые значения 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* $P < \alpha$. Значения α рекомендуется выбирать из интервала $[0{,}001 \div 0{,}01]$.

Например, пусть последовательность S содержит 10^6 бит. Применим к последовательности тест серий, статистикой которого является общее количество серий V, которое в данном случае должно быть близко к значению 500 000. Предположим, что в ходе тестирования мы получили $V = 499996$. Тогда

$$P = erfc\left(\left|\frac{V - 2n\rho(1-\rho)}{2\sqrt{2n}\,\rho(1-\rho)}\right|\right) = 0{,}99487666,$$

где n – длина последовательности; ρ – общее количество единиц, деленное на n; *erfc* – дополнительная функция ошибок.

Поскольку $P > 0{,}01$, то последовательность S тест прошла.

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. Обычно значение вероятности P определяется с использованием

– функции стандартного нормального распределения $\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{\frac{-u^2}{2}}\, du$;

– дополнительной функции ошибок $erfc = \frac{2}{\sqrt{\pi}} \int_{-z}^{\infty} e^{-u^2}\, du$;

– неполной гамма-функции $Q(a,x) \equiv 1 - P(a,x) \equiv \frac{\Gamma(a,x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)} \int_{x}^{\infty} e^{-t} t^{a-1} dt$,

где $Q(a,0) = 1$ и $Q(a,\infty) = 0$.

В основу наиболее мощных библиотек статистического тестирования ГПСЧ, к которым можно отнести пакет DIEHARD [9], Crypt-SX [7] и пакет NIST STS, заложен третий критерий принятия решения.

II Пакет NIST STS

Пакет NIST STS включает в себя 16 статистических тестов, которые разработаны для проверки гипотезы о случайности двоичных последовательностей произвольной длины, порождаемых ГСЧ или ГПСЧ. Все тесты направлены на выявление различных дефектов случайности. Основным принципом тестирования является проверка нулевой гипотезы H_0, заключающейся в том, что тестируемая последовательность является случайной. Альтернативной гипотезой 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, 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 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 $P \geq \alpha$, то гипотеза H_0 принимается. В противном случае принимается альтернативная гипотеза.

Как уже было сказано, пакет включает в себя 16 статистических тестов. Но фактически, в зависимости от входных параметров, вычисляется 189 значений вероятности P, которые можно рассматривать как результат работы отдельных тестов. В таблице 1 приводятся сводные данные по всем тестам с указанием количества вычисляемых значений вероятности P, физического смысла статистики теста и дефекта, на выявление которого направлен тест (в скобках дан порядковый номер теста, который используется на диаграммах).

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Таблица 1

№ п/п	Статистический тест	Количество значений вероятности P	Статистика теста $c(S)$	Выявляемый дефект
1	Частотный (монобитный) тест	1 (1)	Нормализованная абсолютная сумма значений элементов последовательности	Слишком много нулей или единиц в последовательности
2	Частотный тест внутри блока	1 (2)	Мера согласования наблюдаемого количества единиц внутри блока с теоретически ожидаемым.	Локализованные отклонения частоты появления единиц в блоке от идеального значения ½.
3	Проверка накопленных сумм	2 (3-4)	Максимальное отклонение значения накопленной суммы элементов последовательности от начальной точки отсчета (точка 0)	Большое значение единиц или нулей в начале или в конце двоичной последовательности.
4	Проверка серий	1 (5)	Общее количество серий на всей длине последовательности.	Слишком быстрая или слишком медленная перемена знака в ходе генерации последовательности.
5	Проверка максимальной длины серии в блоке	1 (6)	Мера согласования наблюдаемого значения максимальной длины единичной серии с теоретически ожидаемым значением.	Отклонение от теоретического закона распределения максимальных длин серий единиц.
6	Проверка ранга двоичной матрицы	1 (7)	Мера согласования наблюдаемого значения рангов различного порядка с теоретически ожидаемым.	Отклонение эмпирического закона распределения значений рангов матрицы от теоретического, что указывает на зависимость символов в последовательности.
7	Спектральный тест на основе дискретного преобразования Фурье	1 (8)	Нормализованная разница между наблюдаемым и ожидаемым количеством частотных компонент, которые превышают 95 % пороговый уровень.	Выявление периодических составляющих (трендов) в двоичной последовательности.
8	Проверка перекрывающих ся шаблонов	1 (9)	Мера согласования наблюдаемого количества перекрывающихся шаблонов в последовательности с теоретическим значением.	Большое количество m-битных серий из единиц в последовательности.
9	Универсальный тест Маурера	1 (10)	Сумма логарифма расстояния между l-битными шаблонами.	Сжимаемость последовательности.
10	Энтропийный тест	1 (11)	Мера согласования наблюдаемого значения энтропии источника с теоретически ожидаемым для случайного источника.	Неравномерность распределения m-битных слов в последовательности (регулярность свойств источника).
11	Проверка случайных отклонений	8 (12-19)	Мера согласования наблюдаемого количества визитов при случайном блуждании в заданное состояние внутри цикла с	Отклонение от теоретического закона распределения визитов в конкретное состояние при случайном блуждании.

Продолжение таблицы 1

№ п/п	Статистический тест	Количество значений вероятности P	Статистика теста $c(S)$	Выявляемый дефект
			теоретически ожидаемым.	
12	Проверка случайных отклонений (вариант)	18 (20-37)	Общее количество визитов в заданное состояние при случайном блуждании	Отклонение от теоретического ожидаемого общего количества визитов при случайном блуждании в заданное состояние.
13	Последовательный тест	2 (38-39)	Мера согласования наблюдаемого количества всех встретившихся вариантов m-битных шаблонов с теоретически ожидаемым.	Неравномерность распределения m-битных слов в последовательности.
14	Проверка сжатия по алгоритму Лемпеля-Зива	1 (40)	Количество непересекающихся различных слов в последовательности.	Большая степень сжатия тестируемой последовательности по сравнению с ожидаемой степенью сжатия для случайной последовательности.
15	Проверка неперекрывающихся шаблонов	148 (41-188)	Мера согласования наблюдаемого количества непериодических шаблонов в последовательности с теоретическим значением.	Большое количество заданных непериодических шаблонов в последовательности.
16	Проверка линейной сложности	1 (189)	Мера согласования наблюдаемого количества событий, заключающихся в появлении фиксированной длины эквивалентного ЛРР для заданного блока, с теоретически ожидаемым.	Отклонение эмпирического распределения длин эквивалентных ЛРР для последовательности фиксированной длины от теоретического закона распределения для случайной последовательности, что указывает на недостаточную сложность тестируемой последовательности.

Таким образом, в результате тестирования двоичной последовательности формируется вектор значений вероятности $\mathbf{P} = \{P_1, P_2, \ldots, P_{189}\}$. Анализ составляющих P_i данного вектора позволяет указать на конкретные дефекты случайности тестируемой последовательности.

III Методика тестирования генератора

Рассматриваемый 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).

При решении перечисленных задач применяют следующую методику тестирования генераторов.

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 $S = \{s_1, s_2, \ldots, s_n\}$, $s_i \in \{0,1\}$, произвольной длины n.

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

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

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

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

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	$P_{m,1}$	$P_{m,2}$		$P_{m,q}$

$$\Rightarrow \quad \begin{pmatrix} P_{11} & P_{12} & \Lambda & P_{1q} \\ P_{21} & P_{22} & \Lambda & P_{1q} \\ \text{M} & \text{M} & \text{O} & \text{M} \\ P_{m1} & P_{m2} & \Lambda & P_{mq} \end{pmatrix}$$

Введем понятие статистического портрета генератора. *Статистический портрет генератора* представляет собой матрицу размерностью $m \times q$, где m – количество тестируемых двоичных последовательностей, а q – количество статистических тестов, используемых для тестирования каждой последовательности. Элементы матрицы $P_{ij} \in [0,1]$ где $i = \overline{1,m}$, $j = \overline{1,q}$ представляют собой значения вероятности, полученной в результате тестирования i-ой последовательности j-ым 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

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

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

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

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 $k = 1, 2, \ldots, 10$ 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 относительно генератора по следующему решающему правилу: *считается, что генератора 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 $j = \overline{1,q}$.

IV Экспериментальное исследование свойств ГПСЧ

С использованием пакета NIST STS было осуществлено тестирование трех генераторов: генератора псевдослучайных чисел BBS (Blum-Blum-Shub) [10], аппаратного датчика Гряда-1М и генератора на эллиптических кривых (ЭК) [11].

Для осуществления тестирования были выбраны следующие параметры:

1. Длина тестируемой последовательности $n = 10^6$ бит.
2. Количество тестируемых последовательностей $m = 100$. Таким образом, объем тестируемой выборки составил $N = 10^6 \times 100 = 10^8$ бит.
3. Уровень значимости $\alpha = 0{,}01$.
4. Количество тестов $q = 189$. Таким образом, статистический портрет генератора содержит 18900 значений вероятности P.

В идеальном случае при $m = 100$ и $\alpha = 0{,}01$ может быть отвергнута только одна последовательность из ста, т. е. коэффициент прохождения каждого теста должен составлять 99 %. Но это слишком жесткое правило. Поэтому применяется правило на основе доверительного интервала для r_j. Нижняя граница в этом случае составит значение $r_{min} = 0{,}96015$. С этих позиций проанализируем результаты тестирования генераторов, представленные на диаграммах (рис. 1).

В таблице 2 приводятся данные по прохождению генераторами тестов по Правилу 1.

Таблица 2

Генератор	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96%
BBS	134 (70,8 %)	189 (100 %)
Гряда - 1М	130 (68,8 %)	184 (97,4 %)
на ЭК	146 (77,2 %)	188 (100 %)

Аппаратный датчик “Гряда-1М” не прошел пять тестов:

- проверку случайных отклонений – при случайном блуждании часто появляются состояния $x = \{-9, -8, 3, 6\}$;
- проверку не перекрывающихся шаблонов – обнаружено большое количество одного из 148 апериодических шаблонов.

Генератор псевдослучайных чисел на эллиптических кривых не прошел один тест – проверку на не перекрывающиеся шаблоны – обнаружено большое количество одного из апериодических шаблонов.

Генератор BBS прошел все тесты. Но если применить жесткий критерий, т.е. когда может быть отброшена лишь одна последовательность из ста, то лучший результат показал генератор на эллиптических кривых.

В таблице 3 представлены сводные результаты по прохождению генераторами тестов по Правилу 2.

Таблица 3

Генератор	Количество тестов, в которых значение вероятности $P \le 0{,}01$	Количество тестов, у которых значение вероятности $P \le 0{,}001$
BBS	0	0
Гряда - 1М	1	0
на ЭК	3	1

В таблице значения вероятности P сравниваются с уровнями значимости $\alpha = 0{,}01$ и $\alpha = 0{,}001$, т.к. это достаточно малые значения.

Для датчика “Гряда –1М” малое значение вероятности $P = 0{,}0043$ получено для проверки случайных отклонений при $x = -8$ и, таким образом, совпало с низким процентом прохождения последовательностей по данному критерию ($r = 95$ %). Это еще больше свидетельствует о не прохождении генератором данной проверки.

Для генератора на ЭК низкие значения вероятностей получены для:

– проверки случайных отклонений при случайном блуждании $P = 0{,}0033$ для состояния $x = -5$ ($r = 100$ %);

– проверки не перекрывающихся шаблонов $P = 0{,}0043$ ($r = 100$ %)

– критерия на сжатия по Лемпелю-Зиву $P = 0{,}00025$ ($r = 100$ %).

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

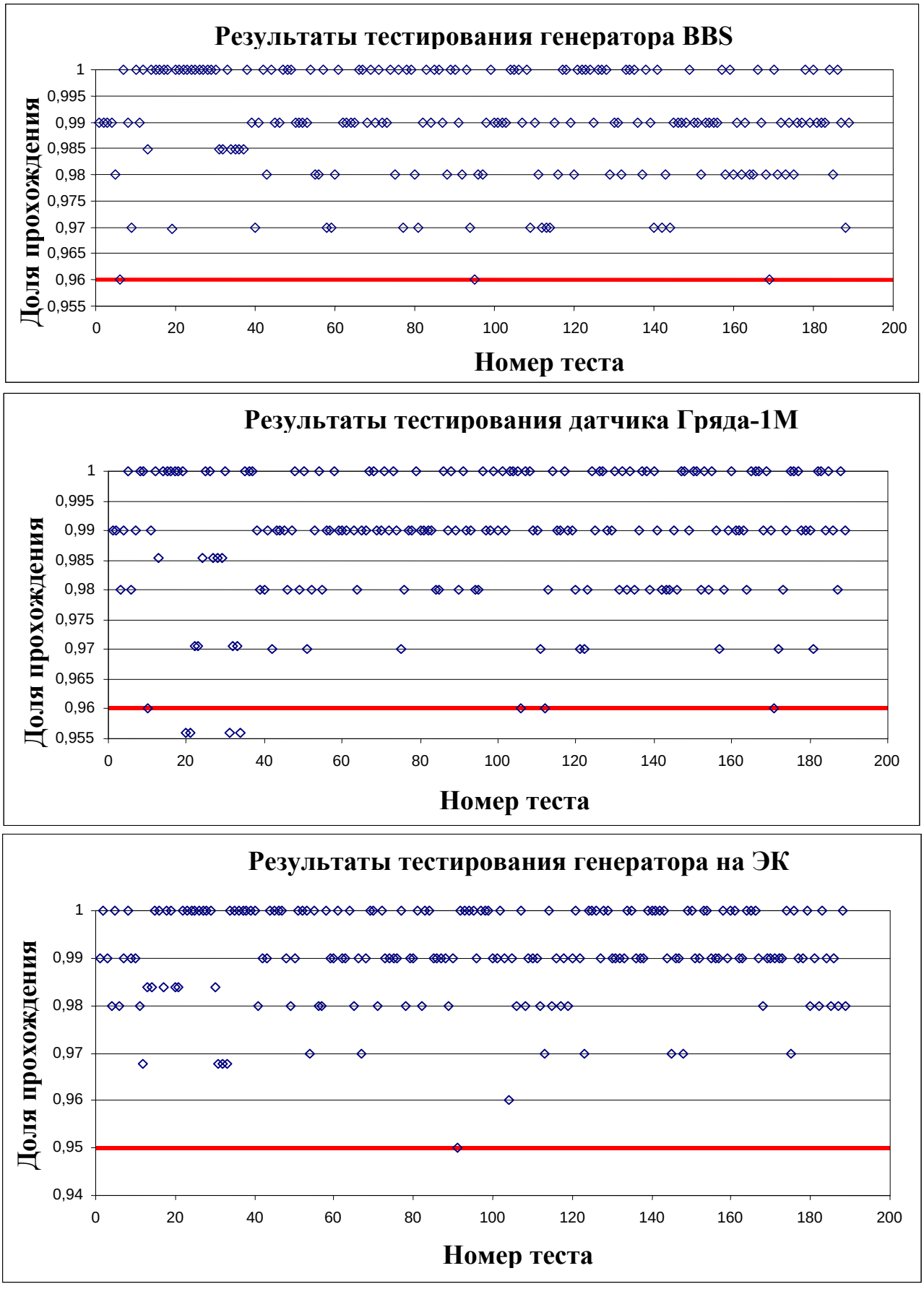

Рисунок 1 – Результаты тестирования генераторов

Таким образом, по правилу два в целом тестирование прошли все генераторы. Однако генератор BBS выглядит предпочтительнее остальных.

Подводя итог тестированию генераторы по убыванию предпочтения можно расставить следующим образом. На первом месте находится генератор BBS, на втором – генератор на основе эллиптических кривых и, наконец, на третьем месте находится аппаратный датчик “Гряда-1М”.

Выводы

Пакет статистических тестов NIST STS является удобным и гибким инструментом исследования ГСЧ (ГПСЧ), применяемых в криптографических приложениях. Данный пакет может и должен быть взят на вооружение отечественными разработчиками соответствующих приложений. В отличие от пакета DIEHARD пакет NIST STS обладает большей гибкостью, расширяемостью и эффективностью (с точки зрения затрачиваемого времени на осуществление тестирования генератора). Кроме того, пакет NIST STS имеет большую криптографическую направленность, которая достигается путем введения в пакет таких тестов, как проверка линейной сложности и универсального теста Маурера.

Рассмотренная методика тестирования и полученные с ее использованием результаты могут рассматриваться как первичный анализ генератора. На основе пакета 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.

Авторы в дальнейшем будут продолжать работы по разработке практических методик применения данного пакета с применением методов ранжирования объектов на основе теории нечетких множеств. Кроме того, представляет интерес сравнение результатов, полученных с использованием пакета NIST STS и пакета DIEHARD, а также выработка рекомендаций по совместному использованию этих пакетов.

Литература: 1. Д. Кнут. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т. 2. – М.: Мир, 1977. – 700 с. 2. Н. П. Бусленко, Д. И. Голенко, И. М. Соболь и др. Метод статистических испытаний (Метод Монте-Карло). – М.: Физматгиз, 1962. – 337 с. 3. Ю. Л Левитан, И. М. Соболь. О датчике псевдослучайных чисел для ПК // Математическое моделирование – 1990. – Т. 2, №8. – С. 119-126. 4. А. В. Потий, А. К. Пестерев. Принципы системного подхода к сертификации генераторов псевдослучайных чисел в системах защиты информации // Радиотехника. Всеукраинский межведомственный научно-технический. сб. 1997. – Вып. 104. – С. 163-172. 5. Security requirements for Cryptographic Modules. FIPS 140-1. – U.S. Department of Commerce. 1994. 6. J. Soto Randomness Testing of the Advanced Encryption Candidate Algorithms. – NIST, 1999. 7. Helen Gustafson, et. al. Statistical test suite Crypt-SX. – Available on http://www.isrc.qut.edu.au/cryptx. 8. A. K. Leung, S. Tavares. Sequence Complexity as Test for Cryptographic Systems. – Advances in Cryptology – CRYPTO’84. Proc. LNCS, Vol. 196 – Springer-Verlag. 9. G. Marsaglia. DIEHARD Statistical Tests. – Available on http://stat.fsu.edu/~geo/diehard.html. 10. Alfred Menezes, et. al. Handbook af Applied Cryptography – CRC Press, 1997. 11. Горбенко Ю. И, Гриненко Т. А., Орлова С. Ю. Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Радиотехника. Всеукраинский межведомственный научно-технический. сб. 2001. – Вып. 119. – С. 163-172.

УДК 681.327.8

ОЦЕНКА СТОЙКОСТИ ПРЕОБРАЗОВАНИЙ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТЫХ ПАРАМЕТРОВ И КЛЮЧЕЙ В КАЧЕСТВЕ ЛИЧНЫХ

Павел Колесников

Харьковский технический университет радиоэлектроники

Аннотация: **Представлены результаты исследования криптографических преобразований в поле эллиптических кривых. Предложена новая схема работы и хранения открытых ключей и параметров в условиях, когда они хранятся в защищенном от внешних пользователей режиме. Даны расчеты стойкости новой схемы работы с ключами.**

 ISBN 966-622-022-9

Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.