УДК 519.246

МЕТОДИКА ТЕСТИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д.Н. Шевченко, С.В. Кривенков

Белорусский государственный университет транспорта, Гомель, Беларусь

TECHNIQUE OF THE TESTING AND USE OF GENERATOR OF PSEUDORANDOM SEQUENCES

D.N. Shevchenko, S.V. Krivenkov

Belarusian State University of Transport, Gomel, Belarus

Рассмотрены существующие подходы к тестированию программных генераторов псевдослучайных последовательностей, их достоинства и недостатки. Предложена методика тестирования нескольких генераторов с целью выбора одного из них для использования в заданной предметной области. Представлены некоторые результаты тестирования наиболее известных генераторов для численного интегрирования методом статистических испытаний Монте-Карло.

***Ключевые слова**: программный генератор случайных чисел, псевдослучайная числовая последовательность, метод Монте-Карло, тестирование на случайность.*

The existing approaches to software testing of pseudorandom sequences, their advantages and disadvantages are reviewed. The methods for testing multiple generators in order to select one of them for use in a certain subject area is offered. Some results of testing famous generators for the numerical integration by Monte Carlo method are shown.

***Keywords**: random number generator, pseudorandom number sequences, Monte Carlo method, testing of pseudorandom sequences.*

Введение

Программные генераторы случайных чисел нашли самое широкое применение от игровой компьютерной индустрии до математического моделирования и криптологии. Основные требования к таким генераторам: независимость элементов генерируемой числовой последовательности, их равномерное распределение на отрезке [0, 1] (т. е. моделирование «базовой» случайной величины), скорость и криптостойкость. Реализуя некоторый алгоритм, программные генераторы вырабатывают числа в зависимости (хотя и неочевидной) от множества предшествующих значений, поэтому полученные числовые последовательности не являются истинно случайными и называются псевдослучайными (ПСП). На данный момент известно более тысячи программных генераторов ПСП, которые различаются алгоритмами и значениями параметров [1]. Существенно различаются и статистические свойства генерируемых ими числовых последовательностей.

1 Обзор подходов к тестированию ПСП

Перед ответственным использованием в математическом моделировании и криптологии программные генераторы ПСП должны быть протестированы. Тесты ПСП условно разделяют на две группы (таблица 1.1).

Эвристические тесты дают, как правило, относительную оценку нескольких альтернативных генераторов (по отношению друг к другу), а статистические тесты выискивают в ПСП детерминированную составляющую и дают абсолютную оценку качества генератора. К сожалению, для многих тестов ПСП присущи следующие ограничения [2]:

1) проверяют лишь одно из вероятностных свойств, характеризующих ПСП;

2) не фиксируют семейство альтернатив;

3) не имеют теоретических оценок мощности.

Таблица 1.1 – Классификация тестов ПСП

1. Эвристические тесты	2. Статистические тесты (критерии)
– проверка скорости; – проверка периода; – на точность определения неких констант (например, числа Пи) методом Монте-Карло; – проверка на криптостойкость; – прочие.	– равномерность распределения; – независимость элементов числовой последовательности; – совпадение числовых характеристик; – комплексные критерии, которые проверяют сразу несколько вышеуказанных требований.

Поэтому для всестороннего и объективного исследования генераторов ПСП необходимо применять сразу множество различных тестов. Определение необходимого и достаточного набора

тестов ПСП представляет пока нерешенную задачу [1], [3]. Другая мало изученная проблема – совместное тестирование нескольких генераторов ПСП используемых, например, для имитационного моделирования систем массового обслуживания [4]. Разработанных статистических тестов в данной области недостаточно.

Особое значение в создании и тестировании программных генераторов ПСП сыграли работы Джорджа Марсальи (1965) [5] и Дональда Кнута (1969) [1], которые предложили целые наборы тестов. Другими стандартными наборами тестов ПСП являются: стандарт NIST STS 800-22 Национального института стандартизации и технологий NIST [6]; стандарт FIPS 140-2 [7]; совокупность статистических критериев, реализованных в пакетах статистического анализа данных, например в Statgraphics. Кроме того, большая группа статистических критериев, пригодных для тестирования ПСП, приводится в справочнике [8]. В публикациях последних лет, например в [9], можно встретить новые оригинальные статистические тесты. Имеются и отечественные тесты ПСП для возможности применения в криптологии [2].

2 Обзор существующих наборов тестов ПСП и их применение

Подборка 14 тестов «Diehard» Дж. Марсальи была первой при комплексном тестировании генераторов ПСП. Подборка рассматривается как одна из наиболее строгих совокупностей тестов; реализована программно и доступна в Интернете [5]. Однако подборка тестов «Diehard» имеет ряд недостатков.

1. Отсутствует подробное описание тестов и методика трактовки результатов [6, с. 159].

2. Параметры тестирования жестко заданы. При этом независимо от длины тестируемой ПСП анализируется только определенное число байт [6, с. 159]. Более короткие ПСП протестировать невозможно.

3. Большинство тестов являются эвристическими и основаны на результатах испытаний, а не на теоретических моделях [6, с. 159].

4. Решение о прохождении теста может принимать только одно из двух значений (да / нет).

Подборка тестов ПСП Д. Кнута использует семь оригинальных статистик и алгоритмов их подсчета. Однако данная подборка имеет ряд недостатков.

1. Все алгоритмы сводятся к вычислению статистических критериев, аппроксимирующихся только распределением χ^2.

2. Отсутствуют рекомендации о параметрах тестирования. Некорректный выбор некоторых значений может привести к существенной зависимости от длины тестируемой последовательности, а также отрицательно сказываться на мощности статистического критерия [6, с.147].

3. Спорной видится [6, с.147] методика оценки результатов, когда случайными признаются последовательности, для которых *P*-value принадлежит интервалу (0,1; 0,9). Т. е. когда *P*-value > 0,9, результаты тестирования считаются слишком идеальными, чтобы считать числовую последовательность случайной.

4. Отсутствует оригинальная программная реализация предложенных тестов.

В работе [3] предлагается набор тестов для предварительной проверки качества случайных чисел и последовательностей на основе семи различных статистических тестов.

Кендэл М. и Смит Б. [10, с. 47] предложили использовать 4 теста с применением критерия χ^2: 1) проверка частоты различных цифр $x_1, x_2, ..., x_N$ в таблице (тест частот); 2) проверка частоты различных двузначных чисел среди пар цифр x_1x_2, x_2x_3, x_3x_4, ..., $x_{N-1}x_N$ (тест пар); 3) проверка частоты различных интервалов между двумя последовательными нулями (тест интервалов); 4) проверка частоты различных типов четверок (*aaaa*, *aaab*, *aabc*, *aabb*, *abcd*) среди четверок $x_1x_2x_3x_4$, $x_2x_3x_4x_5$, $x_3x_4x_5x_6$,..., $x_{N-3}x_{N-2}x_{N-1}x_N$; а также проверка частоты различных типов пятерок (покер-тест).

Стандарт NIST STS 800-22 Национального института стандартизации и технологий NIST [6] включает 15 тестов и ориентирован на тестирование битовых последовательностей, применяемых в задачах криптографической защиты информации.

Типичное применение тестов (в частности, Diehard) приводится, например, в докладе [11].

Таблица 2.1 – Некоторые результаты тестирования генераторов ПСП, применяемых в системах имитационного моделирования GPSS World и AnyLogic

№	Тест	GPSS World		AnyLogic	
1	Дни рождения (Birthday Spacings)	1,000000	–	0,431397	+
2	Пересекающиеся перестановки (Overlapping Permutations)	0,060425	+	0,008494	–
3	Ранги матриц (Ranks of matrices)	0,413445/ 0,536567/ 0,097624	+/+/+	0,382749/ 0,342521/ 0,249165	+/+/+
4	Поток битов (The bitstream test)	1,000000	–	0,482539*	+
5	Обезьяньи тесты (Monkey Tests)	0,585412*	+	0,494274*	+

В таблице 2.1 вещественными числами обозначены *P*-value, которые должны превышать заданный уровень значимости гипотезы о случайности ПСП (по каждому критерию). Однако в докладе [11] спорно используется методика Д. Кнута браковки генераторов. А в некоторых случаях автор ошибочно ищет среднее арифметическое *P*-value по нескольким различным тестам.

При увеличении длины тестируемой ПСП (более 100 тыс.) многие статистические тесты начинают обнаруживать статистически значимые закономерности, которые не обнаруживались на выборках меньшего объема. Так, например, знаковый ранговый критерий (signed rank test, Уилкоксона), который является достаточно мощным [12, с. 223], бракует такие известные и качественные генераторы, как Блюма-Блюма-Шуба (BBS), Шамира (RSA), «Marsaglia Multicarry» и «Xorshift» Джорджа Марсальи, вихрь Мерсенна (MT19937), а также «истинно случайную последовательность» [13] уже на 1,5–2 тысячах элементов числовой последовательности.

Поэтому другой вариант представления результатов тестирования [14] предполагает указание длины битовой ПСП, реализуемой генератором, на которой начинают обнаруживаться статистически значимые признаки неслучайности. В таблице 2.2 символы «–» указывают на то, что за время, отведенное на компьютерный анализ ПСП, статистически значимые закономерности обнаружены не были.

3 Методика тестирования и использования генераторов ПСП в различных предметных областях

Применение каждого из существующих наборов тестов не гарантирует того, что прошедший тесты генератор – качественный. Кроме того, существующие методики тестирования генераторов не дают непосредственного решения двух важных задач:

1) выбор генераторов ПСП (из множества всех доступных генераторов, см. например, таблицу 3.1), которые можно использовать для тех или иных практических целей;

2) ранжирование генераторов по комплексному критерию, учитывающему область практического использования генератора.

Для решения поставленных задач можно предложить методику, включающую следующие положения.

I. При тестировании генераторов ПСП необходимо использовать как можно большее количество известных статистических критериев, отыскивая в ПСП все возможные закономерности. Данное предложение не оригинальное. Так в [7] делается попытка компьютерной реализации всех известных статистических тестов (набор DIEHARD, Д. Кнута, NIST и некоторые другие) для быстрой автоматической проверки генераторов ПСП.

II. Генератор можно использовать, если ни один из используемых статистических критериев не забракует его. При этом, учитывая, что количество тестов имеет порядок 50–70, то используемый уровень значимости должен иметь порядок 0,005–0,015. Увеличение уровня значимости до 0,02 = 1/50 приведет к тому, что в среднем каждый 50-ый тест будет браковать «истинно случайную» последовательность. А уменьшение уровня значимости ниже 0,005 приведет к отказу от браковки «весьма подозрительных» ПСП.

III. Тестирование нескольких генераторов должно проводиться на ПСП одинаковой длины. Это предложение обусловливается тем, что разные по мощности статистические критерии обнаруживают закономерности на числовых последовательностях разной длины.

Таблица 2.2 – Некоторые результаты тестирования генераторов ПСП тестами NIST и тестом «стопка книг» [14]

Генератор/Тест	Стопка книг	6. DFT	11. Serial
24(2, 16598013, 12820163)LCG	2^{16}	2^{21}	2^{23}
31(2, 65539, 0)LCG (RANDU)	2^{13}	2^{22}	2^{20}
32(2, 1099087573, 0)LCG	2^{20}	2^{23}	2^{23}
32(2, 69069, 1)LCG	2^{20}	–	–
32(2, 69069, 5)LCG	2^{20}	–	–
32(2, 1664525, 1013904223)LCG	2^{23}	2^{23}	–
32(2, 22695477, 1)LCG	2^{20}	–	–
32(2, 1103515245, 12345)LCG	2^{23}	–	–
32(2, 134775813, 1)LCG	2^{20}	–	–
32(2, 214013, 2531011)LCG	2^{19}	–	–
RC4	–	–	–
rand (C++ gcc 4.3.2)	–	–	–

Таблица 3.1 – Список основных тестируемых генераторов

1.	Встроенный генератор системы программирования Delphi 2007 (линейный конгруэнтный алгоритм, стартовое значение X_0=1257)
2.	встроенный генератор системы программирования Fortran (линейный конгруэнтный алгоритм, стартовое значение $X_0 = 13$) [1]
3.	Мультипликативный конгруэнтный генератор с параметрами, рекомендованными в книге [Астанин, Л.Ю. Применение программируемых калькуляторов для инженерных и научных расчетов / Л.Ю. Астанин – М.: Энергоиздат, 1986.]
4.	Мультипликативный конгруэнтный генератор RANDU [12, с. 22]
5.	Мультипликативный конгруэнтный генератор ($X_0 = 7$) с параметрами, рекомендованными в книге [12]
6.	Аддитивный генератор Митчелла – Мура (1958) на основе алгоритма Фибоначчи с запаздыванием 55/24 [1, с. 39]
7.	Мультипликативный генератор Марсальи на основе алгоритма Фибоначчи с запаздыванием 55/24 [1, с. 40]
8.	Генератор Левиса-Пэйна (1971) на основе алгоритма Фибоначчи с запаздыванием 55/24 [1, с. 44]
9.	Инверсивный конгруэнтный генератор (Эйченауэра – Лехна) с модулем 2^{31}–1 [1, с. 45]
10.	Аддитивный генератор Фибоначчи с запаздыванием от Беловой с параметрами 97/33 [Белова, И.М. Компьютерное моделирование : учебно-методическое пособие для студентов направления «Прикладная математика и информатика» и «Математическое обеспечение и администрирование информационных систем». / И.М. Белова. – М. : МГИУ, 2007. – 81 с.]
11.	Кубический конгруэнтный генератор [Мартынов, А.И. Методы и задачи криптографической защиты информации : учебное пособие для студентов специальности «Вычислительные машины, комплексы, системы и сети» / А.И. Мартынов. – Ульяновск : УлГТУ, 2007. – 92 с.]
12.	MWC1616 – конкатенация двух 16-битных генераторов [5]
13.	Генератор «Xorshift» [5]
14.	Генератор «multiply-with-carry» [5]
15.	Генератор «Marsaglia Multicarry» [5]
16.	Генератор «MotherOfAll» [5]
17.	Комбинация Xor-Shift, линейного конгруэнтного и метода Фибоначчи [5]
18.	Генератор «COMBO» [5]
19.	Генератор «ULTRA» [5]
20.	Генератор «KISS» [5]
21.	Вихрь Мерсенна MT19937 ($123, $234, $345, $456) [Makoto Matsumoto, Takuji Nishimura, «Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator», ACM Transactions on Modeling and Computer Simulation (TOMACS), 8:1, jan. (1998), 3–30]
22.	Комбинация трех мультипликативных конгруэнтных генераторов от Б. Уичмана и И. Хилла (1982) [12, с. 22]
23.	Генератор Экуйера на основе двух мультипликативных конгруэнтных генераторов [Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с., с. 276]
24.	Генератор Блюм-Блюма-Шуба с $p = 12647$, $q = 12659$, $X_0 = 127$ [6]
25.	Генератор Макларена – Марсальи [1] на основе двух линейных конгруэнтных генераторов
26.	Генератор Макларена – Марсальи [1] на основе генератора «multiply-with-carry» и линейного конгруэнтного генератора (размер массива 256 чисел; адрес выбирается битами 9–16 числа Y_0)
27.	Истинно случайная последовательность из книги [13]

IV. За прохождение каждого теста генератору ПСП назначают «балл», характеризующий качество генератора по данному критерию. Для статистических критериев таким баллом может быть значение P-value $\in [0, 1]$, характеризующее вероятность того, что «ПСП неслучайна».

Использование баллов позволяет сравнивать результаты тестирования генераторов ПСП по нескольким различным тестам, причем в одинаковой количественной шкале.

V. Каждому тесту назначают «значимость» – важность для той или иной предметной области. Например, в криптологии наиболее высоки требования к «криптостойкости» генератора, а в имитационном моделировании – к «совпадению моментов» ПСП.

VI. Выбор генератора ПСП для использования в той или иной области определяется суммой баллов, набранных по различным тестам, нормированных их значимостью для данной предметной области.

Таблица 3.1 – Результаты тестирования генераторов RANDU и Marsaglia Multicarry с учетом баллов

Генераторы:		31(2,65539,0)LCG (RANDU)			Marsaglia Multicarry		
Тесты	Значи-мость	Результат	Балл	Взвеш. балл	Результат	Балл	Взвеш. балл
1. Эвристические тесты							
Период	8	Более 300 млн	8	64	Более 300 млн	9	72
Время генерации 1 млн. элементов	5	894,4 мс	7	35	873,7 мс	8	40
2. Статистические тесты Statgraphics Centurion							
2.1. Критерий Стьюдента (t-test)	9	$P=0{,}28$	6	54	$P=0{,}54$	8	72
2.2. Знаковый критерий (sign test)	6	$P=0{,}59$	8	48	$P=0{,}64$	8	48
2.3. Критерий согласия χ^2 Пирсона	9	$P=0{,}49$	8	72	$P=0{,}63$	8	72
2.4. Тест Бокса-Пирса	6	$P=0{,}55$	8	48	$P=0{,}08$	3	18
… всего 16 тестов							
3. Тесты Д. Кнута							
3.1. Тест интервалов (0,2, 0,5)	5	1,49<12,6	9	45	6,7<12,6	7	35
3.2. Тест непересекающихся перестановок	5	20,2<35,2	6	30	12,87<35,2	7	35
… всего 7 тестов							
4. Тесты «DIEHARD» Дж. Марсальи							
4.1. Тест пересекающихся перестановок	7	29,9<35,2	5	35	17,6<35,2	6	42
4.2. Тест «крэпс»	7	8,5<12,6	5	35	$13{,}3 \notin (0;\ 12{,}6)$	1	7
… всего 14 тестов							
5. Тесты NIST							
5.1. Частотный монобитный тест	6	$1{,}83 \in (-1{,}96;\ 1{,}96)$	4	24	$1{,}42 \in (-1{,}96;\ 1{,}96)$	6	36
… всего 16 тестов							
6. Общие статистические тесты							
6.1. Критерий серий	4	$1{,}59 \in (-1{,}96;\ 1{,}96)$	5	20	$0{,}89 \in (-1{,}96;\ 1{,}96)$	7	28
6.2. Критерий инверсий	5	$0{,}02 \in (-1{,}96;\ 1{,}96)$	8	40	$0{,}000138 \in (-1{,}96;\ 1{,}96)$	9	45
6.3. Критерий длин восходящих и нисходящих серий	5	$49{,}1 \notin (0;\ 5{,}99)$	0	0	$27{,}8 \notin (0,\ 5{,}99)$	1	5
6.4. Критерий согласия Морана	8	$-2{,}27 \notin (-1{,}96;\ 1{,}96)$	1	8	$-1{,}19 \in (-1{,}96;\ 1{,}96)$	6	48
6.5. Критерий серий Вальда – Волфовица	8	$-0{,}03 \in (-1{,}96;\ 1{,}96)$	8	64	$0{,}009 \in (-1{,}96;\ 1{,}96)$	8	64
6.6. Тест χ^2 на равномерность двумерного распределения	9	7,69<25,0	6	54	8,99<25,0	5	45
6.7. Тест χ^2 на равномерность трехмерного распределения	9	19,3<23,7	5	45	13,0<23,7	6	54
… всего 31 тест							
ИТОГО баллов по представленным тестам				721			766

В различных предметных областях перед генераторами ПСП стоят различные задачи. Так в некоторых задачах компьютерного моделирования важно, чтобы ПСП в основном удовлетворяла тестам на «совпадение моментов», в других задачах – тестам на отсутствие авто- и взаимной корреляции, в третьих – на равномерность. Поэтому для решения различных задач следует применять различные генераторы ПСП, которые для данной группы задач набирают больше баллов, нормированных значимостью соответствующих тестов.

Не претендуя на окончательную объективность, представим таблицу баллов и значимости некоторых тестов для целей использования генераторов ПСП при решении задач численного интегрирования методом статистических испытаний Монте-Карло (таблица 3.1) на примере генераторов RANDU и Marsaglia Multicarry.

В примере, представленном в таблице 3.1, подсчет суммы баллов с учётом значимости тестов показал, что генератор «Marsaglia Multicarry» набрал большее количество баллов, чем генератор «RANDU», поэтому он может быть признан более целесообразным для использования в данной предметной области.

VII. Тестирование нескольких генераторов в совокупности имеет важное значение. При моделировании обычно используется несколько генераторов. При этом может оказаться, что получаемые ими числовые последовательности коррелированны. Это приведет к тому, что полученные результаты моделирования будут не корректны.

При совместном использовании нескольких генераторов ПСП необходимо дополнительное тестирование генераторов с определением характеристик, список которых на данный момент не разработан [4]. Здесь видится возможным применение статистических критериев с оценкой взаимной корреляционной функции, а также эвристический тест на оценку длины очереди системы массового обслуживания $M/M/1$ с как можно большей точностью.

Заключение

Таким образом, в работе предложена методика тестирования генераторов ПСП и формальный количественный критерий для выбора одного из нескольких доступных генераторов ПСП.

Для реализации предлагаемого подхода авторами разрабатывается программный комплекс тестирования генераторов ПСП, который будет включать в себя все известные статистические и эвристические тесты. Комплекс базируется на табличном процессоре Microsoft Excel, что обусловлено большим количеством встроенных математических и статистических функций, возможностью программирования на VBA, а также наглядностью реализации и тестирования программ, созданных несколькими авторами. В настоящее время реализовано более 45 тестов ПСП, и база тестов пополняется.

В результате реализации данной методики будет создана информационная система, которая позволит выбирать качественный программный генератор ПСП для использования в той или иной предметной области.

ЛИТЕРАТУРА

1. *Кнут*, *Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. / Д. Кнут. – 3-е изд. – М.: Вильямс, 2000. – 832 с.

2. *Харин*, *Ю.С.* Проверка гипотез о независимости и равномерном вероятностном распределении элементов случайной последовательности / Ю.С. Харин, А.И. Петлицкий // Вестник БГУ. Серия 1. – 2007. – № 3. – С. 74–80.

3. *Акимова*, *Г.П.* Методологический подход к оценке качества случайных чисел и последовательностей / Г.П. Акимова, Е.В. Пашкина, А.В. Соловьев // Труды ИСА РАН. – 2008. – Т. 38. – С. 156–167.

4. *Алиев*, *Т.И.* Проблема сочетания генераторов псевдослучайных величин в GPSS-моделях / Т.И. Алиев, Г.К. Асафьев // Пятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика (ИММОД-2011)». – Санкт-Петербург. – 2011. – Т. 1. – С. 95–100.

5. *Marsaglia*, *G.* The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, дата обращения 14 января 2013, Электронный ресурс: http://www.stat.fsu.edu/pub /diehard.

6. *Иванов*, *М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с.

7. *Вильданов*, *Р.Р.* Тесты псевдослучайных последовательностей и реализующее их программное средство / Р.Р. Вильданов, Р.В. Мещеряков, С.С. Бондарчук // Доклады ТУСУРа, № 1 (25), Ч. 2., июнь 2012. – С. 108–111.

8. *Кобзарь*, *А.И.* Прикладная математическая статистика: для инженеров и научных работников / А.И. Кобзарь. – М. : Физматлит, 2006. – 813 с.

9. *Рябко*, *Б.Я.* «Стопка книг» как новый статистический тест для случайных чисел / Б.Я. Рябко, А.И. Пестунов // Проблемы передачи информации. – 2004. –Т. 40, вып. 1. – С. 73–78.

10. *Иванова*, *В.М.* Случайные числа и их применение. – М. : Финансы и статистика, 1984. – 111 с.

11. *Диденко*, *Д.Г.* Качество генерации псевдослучайных чисел в системах имитационного моделирования OpenGPSS, GPSS World и AnyLogic / Д.Г. Диденко // Пятая всероссийская научно-практическая конференция по имитационному

моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика (ИММОД-2011)». – Санкт-Петербург. – 2011. – Т. 1. – С. 134–138.

12. *Лагутин*, *М.Б.* Наглядная математическая статистика : учебное пособие / М.Б. Лагутин. – 2-е изд., испр. – М. : БИНОМ. Лаборатория знаний, 2009. – 472 с.

13. *The RAND Corporation.* A Million Random Digits with 100 000 Normal Deviates. – N.Y. : Free Press, 1966.

14. *Миненко*, *А.И.* Экспериментальное исследование эффективности тестов для проверки генераторов случайных чисел / А.И. Миненко // Вестник СибГУТИ. – 2010. – № 4. – С. 36–46.

Поступила в редакцию 23.12.13.