УДК 004.056 : 519.2
Фауре Э.В, Щерба А.И., Лавданский А.А
Черкасский государственный технологический университет

ОЦЕНКА СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ПОСЛЕДОВАТЕЛЬНОСТИ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ПОРОЖДЕННОЙ КОМБИНАЦИОННЫМ ГЕНЕРАТОРОМ

Фауре Э.В., Щерба А.И., Лавданский А.А. Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором Генераторы псевдослучайных последовательностей находят применение для решения широкого круга практических задач. Однако последовательности псевдослучайных чисел не могут быть использованы без детального исследования статистических свойств и сравнительных количественных оценок. В работе рассмотрен комбинационный метод генерации псевдослучайных чисел. Рассмотрены способы построения исходных таблиц для комбинационного генератора с помощью существующих генераторов псевдослучайных и случайных чисел. Проведен анализ статистических характеристик последовательности чисел на выходе комбинационного генератора с помощью специализированного пакета тестирования NIST. Произведена оценка исследуемых последовательностей с помощью непараметрических критериев, таких как критерий знаков и критерий серий. Результаты, полученные в работе, позволяют использовать комбинационный генератор в задачах, требующих высокого качества последовательностей псевдослучайных чисел.
Ключевые слова: последовательность псевдослучайных чисел, комбинационный генератор, тестирование, непараметрический критерий.

Фауре Е.В., Щерба А.І., Лавданський А.О. Оцінка статистичних характеристик послідовності псевдовипадковихчисел, що породжена комбінаційним генератором Генератори псевдовипадкових послідовностей знаходять застосування для вирішення широкого кола практичних задач. Однак послідовності псевдовипадкових чисел не можуть бути використані без детального дослідження статистичних властивостей і порівняльних кількісних оцінок. У роботі розглянуто комбінаційний метод генерації псевдовипадкових чисел. Розглянуто способи побудови вихідних таблиць для комбінаційного генератора за допомогою існуючих генераторів псевдовипадкових і випадкових чисел. Проведено аналіз статистичних характеристик послідовності чисел на виході комбінаційного генератора за допомогою спеціалізованого пакета тестування NIST. Проведена оцінка досліджуваних послідовностей за допомогою непараметричних критеріїв, таких як критерій знаків і критерій серій.Результати, отримані в роботі, дозволяють використовувати комбінаційний генератор в задачах, що потребують високої якості послідовностей псевдовипадкових чисел.
Ключові слова: послідовність псевдовипадкових чисел, комбінаційний генератор, тестування, непараметричний критерій.

E. Faure, A. Shcherba, A. Lavdanskiy Cherkasy state technological university Estimation of statistical characteristics for pseudorandom numbers sequence generated by combinational generator Generators of pseudorandom sequences are used for a wide range of practical problems. However, the sequence of pseudorandom numbers can not be used without detailed study of the statistical properties of the comparative and quantitative assessments. In this paper we consider the combinational method of pseudorandom numbers generating. Methods of constructing the source tables for combinational generator with existing generators of pseudorandom and random numbers are reviewed. The analysis of the statistical characteristics of the output numbers sequence of combinational generator using specialized test suite NIST is performed. The estimation of the test sequences using nonparametric tests such as the sign test and runs test is performed. The results obtained in this work allow the use of the combinational generator in tasks requiring high quality of pseudorandom numbers.
Keywords: pseudorandom numbers sequence, combinational generator, testing, nonparametric test.

Введение

Генераторы псевдослучайных чисел (ПСЧ) широко используются для решения большого круга практических задач, таких как задачи защиты информации, имитационного моделирования и т.д. При этом результат решения задачи значительно зависит от качества используемого генератора. Качественный генератор ПСЧ должен производить последовательность чисел, сравнимую по своим статистическим характеристикам с последовательностью случайных чисел, порождаемых естественными (природными) источниками, и при этом быть воспроизводимым. Существующие генераторы ПСЧ обладают многими характеристиками естественных источников случайных чисел, но на данный момент времени не существует генератора ПСЧ, неотличимого по своим статистическим характеристикам от естественных генераторов случайных чисел (ГСЧ). Поэтому задача улучшения качества генераторов ПСЧ и поиска новых алгоритмов формирования ПСЧ является актуальной и стимулирует исследования путей улучшения статистических свойств псевдослучайных последовательностей чисел.

Постановка проблемы

Различные методы генерации псевдослучайных чисел не могут быть применены для решения практических задач без исследования их статистических свойств и сравнительных количественных оценок. Для исследования статистических свойств используют различные статистические тесты, объединенные в пакеты тестирования. Прохождение статистических тестов позволяет с высокой вероятностью говорить о высоком качестве исследуемой псевдослучайной последовательности чисел.

Целью настоящей работы является оценка качества последовательности псевдослучайных чисел, порожденных комбинационным генератором, с помощью статистических пакетов тестирования, а также некоторых непараметрических критериев.

Постановка задачи

Комбинационные генераторы, подробно рассмотренные в [1, с. 45-49] и [2, с. 283-290], основываются на комбинации нескольких исходных генераторов. Такие генераторы позволяют улучшить статистические свойства последовательностей на выходе существующих генераторов псевдослучайных чисел. Кроме того, комбинация генераторов позволяет увеличить период повторения последовательности.В данной работе будем рассматривать комбинационный генератор с различным количеством исходных генераторов (от 2 до 8), представляющих собой циклические сдвиговые регистры (таблицы) с записанными в них перестановками, сформированными с помощью линейного конгруэнтного метода [2, с. 275-277], аддитивного генератора [3] либо генератора случайных чисел (в данной работе используется квантовый ГСЧ [4]). Мощность алфавита M выбрана равной 256, что позволяет без дополнительных преобразований формировать бинарный файл из слов на выходе комбинационного генератора, пригодный для последующего использования статистическими пакетами тестирования.

Комбинирующей функцией рассматриваемого генератора является функция "сумма по модулю M", применяемая к значениям последовательностей, порожденных группой независимых первичных генераторов.Задачей работы является исследование статистических характеристик последовательностей, порождаемых комбинационным генератором с комбинирующей функцией суммы по модулю M в зависимости от количества исходных таблиц перестановок и их заполнения.

Решение задачи

Алгоритм работы рассматриваемого в данной работе комбинационного генератора изложен в [5]. Его принцип работы состоит в следующем. Группа исходных генераторов работает синхронно (слова на выходе каждого из генераторов появляются одновременно). В исходные генераторы (таблицы перестановок) записаны перестановки на множествах с мощностями алфавитов M_i (последовательности чисел, которые равномерно распределены на отрезке $[0, M_i-1]$ с нулевой ошибкой воспроизведения [6]). Результаты работы каждого из генераторов одновременно подаются на вход сумматора по модулю M, выход которого и является результатом работы комбинационного генератора.

Предположим, что $X_1, X_2, \ldots, X_n$ – дискретные равномерно распределенные случайные величины в диапазоне $[0..M-1]$. Широко известно, что случайная величина $Y = |X_1 + X_2 + \ldots + X_n|_M$ – также равномерно распределена в диапазоне $[0..M-1]$. Такое утверждение справедливо также для бесконечных последовательностей значений случайных величин $X_1, X_2, \ldots, X_n$.

Если исходные последовательности $X_1, X_2, \ldots, X_n$ представляют собой циклически повторяющиеся перестановки на множествах с мощностями алфавитов M_i, следует воспользоваться результатами исследования, изложенного в [7]. Пусть каждый из двух исходных генераторов циклически формирует некоторую перестановку на множествах целых чисел из диапазонов $[0, M_1 - 1]$ и $[0, M_2 - 1]$ для первого и второго генератора, соответственно. Тогда, как указано в [7], для равномерного распределения дискретной случайной величины на множестве целых чисел мощности M на выходе комбинационного генератора, выполняющего операцию суммирования по модулю M слов от двух исходных генераторов, достаточно, чтобы M_1 и M_2 были взаимно просты и одно из значений M_1 или M_2 было кратно M .

Указанное утверждение с помощью метода индукции можно расширить для комбинационного генератора, состоящего из n исходных генераторов. В результате получим утверждение: для равномерного распределения дискретной случайной величины на множестве целых чисел мощности M на выходе комбинационного генератора, выполняющего операцию суммирования по модулю M слов от n исходных генераторов, где i-ый исходный генератор

циклически формирует некоторую перестановку на множестве целых чисел из диапазона $[0, M_i - 1]$, $i \in [1, n]$, достаточно, чтобы все значения M_i были попарно взаимно просты $\left(НОД\left(M_i, M_j\right)\Big|_{i \neq j} = 1 \right)$ и одно из значений M_i было кратно M.

Следует учитывать, что период комбинационного генератора будет равен наименьшему общему кратному периодов исходных генераторов. При использовании исходных генераторов (таблиц перестановок) с взаимно простыми периодами повторения можно достичь максимального периода последовательности на выходе комбинационного генератора $T_{\max} = \prod_i M_i$.Комбинационный генератор позволяет использовать существующие методы формирования псевдослучайных чисел, такие как линейный конгруэнтный метод или метод, основанный на использовании регистра сдвига с обратными связями, без их дополнительной модернизации.

В целях ускорения работы и упрощения конструкции рассматриваемого комбинационного генератора будем рассматривать предварительно подготовленные таблицы перестановок (исходные таблицы), сформированные с помощью генераторов псевдослучайных либо случайных последовательностей.

Заполнение исходных таблиц перестановок комбинационного генератора

Существуют два принципиально разных типа генераторов случайных и псевдослучайных чисел. Для пояснения рассмотрим аналогию с лототроном, в который засыпаны пронумерованные от *0* до *M*-1 шары.

Если последовательно извлекать перемешанные шары из урны, не возвращая шар в урну, получим генератор типа "без возврата". Вероятность выпадения каждого шара для этого типа генераторов зависит от порядкового номера вытянутого шара и равна $p_i = \frac{1}{M - i}$, где i – порядковый номер шара, $i \in [0, M\text{-}1]$. После опустошения урна снова засыпается шарами, они перемешивается, а приведенный алгоритм повторяется.

Тип генератора "с возвратом" отличается от описанного выше тем, что извлеченный шар после считывания его численного значения, опускается в урну и шары в урне повторно перемешиваются. Вероятность выпадения шара в таком случае не зависит от порядкового номера шара и равна $p_i = \frac{1}{M}$.Для формирования исходных таблиц комбинационного генератора при использовании генераторов случайных чисел возникает проблема повторения слов в таблицах. Поскольку генератор случайных чисел работает по схеме "с возвратом", а $p_i = \frac{1}{M}$, его использование в исходном виде для заполнения таблиц в комбинационном генераторе не представляется возможным. Рассмотрим алгоритм построения исходных таблиц для комбинационного генератора с помощью генераторов (псевдо)случайных чисел, функционирующих по схеме "с возвратом", т. е. алгоритм преобразования генератора "с возвратом" в генератор "без возврата".

Сформируем две пустые таблицы *A* и *B* размером *M*, где *M* – мощность алфавита требуемой таблицы. Таблица *A* – временная таблица, таблица *B* – таблица-результат. Заполним таблицу *A* последовательно значениями от 0 до *M*-1. Генератор типа "с возвратом" (далее генератор) настроим на формирование числа в диапазоне от 0 до *M*-1. Значение, полученное от генератора, является указателем на ячейку таблицы *A*. Значение этой ячейки записывается в таблицу *B* на нулевую позицию. Из таблицы *A* ячейка удаляется со сдвигом всех последующих значений вверх и уменьшением размера таблицы на единицу. Далее генератор настраивается на формирование числа в диапазоне от 0 до *M*-2 (где *M*-2 фактически является новым размером таблицы *A*). Полученное значение аналогично используется как указатель в таблице *A* с последующим перемещением ячейки таблицы *A* на следующую позицию таблицы *B*. После *M* итераций описанного алгоритма в таблице *B* находятся значения от *0* до *M*-1 без повторов и пропусков, перемешанные соответственно использованному генератору.

Статистические свойства последовательности, порожденной комбинационным генератором

Для определения статистических свойств случайных и псевдослучайных последовательностей чисел применяются различные тесты, из которых можно выделить два класса: статистические и графические [8]. Статистические тесты позволяют получить численную оценку качества исследуемой последовательности. Результат графического теста представляется в виде графика и не имеет численного значения, является субъективным и не может быть объективно оценен.Существует множество пакетов статистического тестирования последовательностей чисел, такие как: тесты NIST, DIEHARD, TEST-U01, CRYPT-X, The pLab Project, Dieharder, ENT и др. В данной работе используется пакет тестирования NIST [9] как наиболее подробно отражающий статистические характеристики исследуемых последовательностей.

Дополнительно проведем оценку последовательности на выходе исследуемого генератора с помощью непараметрических критериев, таких как критерий знаков [10, с. 254-260, 11, с. 89-91] и критерий серий [11, с.91-93]. Заметим, что непараметрические критерии используют не численные значения выборки, а ее структурные свойства, что позволяет провести оценку последовательности независимо от предполагаемого закона распределения.Так, критерий знаков позволяет определить однородность двух рассматриваемых выборок. Однородными называются выборки, имеющие равные функции распределения. В данной работе будем рассматривать сравнение различных реализаций комбинационного генератора со случайной последовательностью чисел.Критерий серий позволяет определить, что слова на выходе исследуемого генератора являются случайными и независимыми.

Результаты анализа последовательности с помощью пакета тестирования NIST

Для определения статистических характеристик использовалась выборка размером 2^{25} байт. Каждый из 188 тестов пакета производится N раз над последовательностью длиной V бит. В данной работе, в соответствии с рекомендациями NIST [9], N=100, V=1000000. В качестве нулевой гипотезы H_0 принималась гипотеза о том, что проверяемая последовательность является случайной. Результатом работы каждого теста является N значений, называемых *p-value*. *P-value* есть вероятность ошибки при отклонении нулевой гипотезы о случайности последовательности (ошибка первого рода). N результатов тестов разделяются по значению на 10 групп: [0;0,1), [0,1;0,2), …, [0,9;1]. Распределение по этим группам должно быть равномерным. Подсчитанное количество значений в каждой из групп оцениваются с помощью критерия хи-квадрат (теоретическое значение N/10). Полученная оценка и является результатом каждого из тестов пакета. Результаты тестирования по этому параметру приведены в таблице 1.

Таблица 1

Количество тестов, не удовлетворяющих доверительной вероятности для теста NIST

Заполнение таблиц	Количество исходных таблиц						
	2	3	4	5	6	7	8
Линейный конгруэнтный метод	148/188	1/188	0/188	0/188	0/188	0/188	0/188
Аддитивный генератор	147/188	0/188	0/188	0/188	0/188	0/188	0/188
Квантовый генератор случайных чисел	149/188	0/188	0/188	0/188	0/188	0/188	0/188

Дополнительно производится подсчет полученных значений *p-value*, не удовлетворяющих доверительной вероятности. В данной работе доверительная вероятность равна $\alpha=0,01$. Отношение количества значений *p-value*, которые больше доверительной вероятности, к общему количеству результатов теста отображается в процентном соотношении. В соответствии с рекомендациями NIST [9], в данной работе используется ограничение в 96% – тесты с меньшим значением считаются не пройденными. Результаты тестирования по этому параметру приведены в таблице 2.

Таблица 2

Количество тестов, в которых тестирование прошло меньше 96% последовательностей для теста NIST

Заполнение таблиц	Количество исходных таблиц						
	2	3	4	5	6	7	8

Линейный конгруэнтный метод	11/188	1/188	2/188	1/188	3/188	1/188	3/188
Аддитивный генератор	17/188	3/188	2/188	0/188	0/188	0/188	0/188
Квантовый генератор случайных чисел	20/188	1/188	1/188	0/188	0/188	0/188	0/188

Рассмотрим результаты статистического исследования последовательностей с помощью пакета NIST. Как следует из таблиц 1 и 2, при использовании двух исходных таблиц в независимости от метода их заполнения видно, что большая часть тестов не удовлетворяет доверительной вероятности (таблица 1), а также значительная часть тестов не преодолевает порог пройденных тестов в 96% (таблица 2). Причины таких результатов следующие. При использовании двух исходных таблиц в данной работе использовались таблицы размерами $M_1 = 251$ и $M_2 = 241$ для всех вариантов заполнения. При такой конфигурации комбинационного генератора период формируемой им последовательности равен $T = M_1 * M_2 = 251 * 241 = 60491$ слов или 483928 бит. При этом, согласно рекомендациям, изложенным в [9], исследования проводились для последовательностей длиной 1000000 бит. В случае с двумя исходными таблицами происходит зацикливание генератора, которое ведет к повторению последовательности после 483928 бит. Естественно такая последовательность не может считаться случайной, что и определяет данный статистический пакет тестирования. Поэтому следует всегда учитывать период повторения последовательности на выходе комбинационного генератора при его использовании.

При использовании трех и более исходных таблиц все варианты заполнения комбинационного генератора удовлетворят требованиям доверительной вероятности (таблица 1). Однако дополнительная оценка по проценту последовательностей, прошедших тесты (таблица 2), показывает незначительные отклонения для последовательностей при заполнении исходных таблиц с помощью линейного конгруэнтного метода. При таких результатах тестирования не рекомендуется использовать подобную конструкцию комбинационного генератора в задачах, требующих высокого качества псевдослучайных последовательностей. Для других же вариантов заполнения исходных таблиц (при количестве таблиц 5 и более) последовательности полностью проходят все тесты пакета тестирования NIST, что свидетельствует о высоком качестве последовательности псевдослучайных чисел, получаемой на выходе комбинационного генератора.

Результаты анализа последовательности с помощью непараметрических критериев знаков и серий

Рассмотрим результаты исследования последовательностей, порожденных комбинационным генератором, с помощью критерия знаков.В качестве эталонной последовательности использована случайная последовательность чисел, полученная с помощью [12]. В качестве основной гипотезы H_0 принимается утверждение, что исследуемые последовательности являются однородными, т.е. вероятности отклонения разности между словами исследуемой и случайной последовательностей в ту либо иную сторону равны между собой. Тогда H_0: $p = ½$. В качестве альтернативных выдвигаются гипотезы:

– гипотеза H_1: $p > ½$ – вероятность отклонения разности между словами исследуемой и случайной последовательностей в положительную сторону больше, чем в отрицательную;

– гипотеза H_2: $p < ½$ – вероятность отклонения разности между словами исследуемой и случайной последовательностей в отрицательную сторону больше, чем в положительную.

Если результат $F_в$ расчетного значения статистики критерия знаков меньше критического значения F-распределения Фишера ($F_в < F_{(1-\alpha)}(k_1,k_2)$) – тест считается пройденным. Для данного критерия в работе используется уровень значимости $\alpha = 0,05$.В соответствии с рекомендациями, изложенными в [10, с. 257-258], число испытаний для применения критерия знаков должно быть достаточно велико для значений p, близких к ½ и конкурирующих с $p = ½$. Так, например, для того, чтобы критерий знаков в 95% случаев отбрасывал гипотезу H_0: $p = ½$, когда на самом деле $p=0,45$ с уровнем значимости $q=5\%$, необходимо произвести не менее 1297 наблюдений [10, с. 258]. Минимальный требуемый объем выборки монотонно увеличивается при приближении значения p к ½ и при уменьшении уровня значимости q. Исходя из этого, в качестве исходных данных для применения критерия знаков в настоящей работе рассматривались первые 4096 слов каждой из последовательностей комбинационного генератора в зависимости от различного количества исходных таблиц и различного их заполнения. Результаты исследования приведены в таблицах 3, 4, 5.

Таблица 3

Результаты теста критерия знаков для заполнения исходных таблиц с помощью аддитивного генератора

Количество исходных таблиц	$H_1 : p > 1/2$				$H_2 : p < 1/2$			
	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$
2	4004	4158	1,03846	1,052845	4160	4002	0,96202	1,052877
3	4120	4030	0,97816	1,052903	4032	4118	1,02133	1,052885
4	4048	4118	1,01729	1,052833	4120	4046	0,98204	1,052847
5	4064	4092	1,00689	1,052868	4094	4062	0,99218	1,052874
6	4086	4072	0,99657	1,052866	4074	4084	1,00245	1,052863
7	4150	4006	0,9653	1,052894	4008	4148	1,03493	1,052865
8	4170	4004	0,96019	1,052839	4006	4168	1,04044	1,052806

Таблица 4

Результаты теста критерия знаков для заполнения исходных таблиц с помощью линейного конгруэнтного метода

Количество исходных таблиц	$H_1 : p > 1/2$				$H_2 : p < 1/2$			
	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$
2	4032	4126	1,02331	1,052858	4128	4030	0,97626	1,052878
3	4144	4012	0,96815	1,052891	4014	4142	1,03189	1,052865
4	4042	4110	1,01682	1,052879	4112	4040	0,98249	1,052893
5	4104	4058	0,98879	1,052856	4060	4102	1,01034	1,052847
6	4106	4050	0,98636	1,052878	4052	4104	1,01283	1,052867
7	4136	4018	0,97147	1,052895	4020	4134	1,02836	1,052871
8	4136	4032	0,97485	1,052846	4034	4134	1,02479	1,052825

Таблица 5

Результаты теста критерия знаков для заполнения исходных таблиц с помощью квантового генератора случайных чисел

Количество исходных таблиц	$H_1 : p > 1/2$				$H_2 : p < 1/2$			
	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$	k_1	k_2	$F_в$	$F_{(1-\alpha)}(k_1,k_2)$
2	4178	3990	0,955	1,052864	3992	4176	1,04609	1,052826
3	4112	4060	0,98735	1,052824	4062	4110	1,01182	1,052814
4	4030	4108	1,01935	1,052925	4110	4028	0,98005	1,052942
5	4144	4010	0,96766	1,052898	4012	4142	1,0324	1,052871
6	4120	4044	0,98155	1,052854	4046	4118	1,0178	1,052839
7	4150	4006	0,9653	1,052894	4008	4148	1,03493	1,052865
8	4000	4166	1,0415	1,052832	4168	3998	0,95921	1,052866

Результаты исследование с помощью критерия знаков показывают однородность последовательности, полученной с помощью комбинационного генератора (при исследованных вариантах заполнения исходных таблиц), и последовательности случайных чисел. Из этого можно сделать вывод, что функции распределения исследуемых случайных величин равны.Результаты исследования последовательностей, сформированных комбинационным генератором, с помощью критерия серий приведены в таблице 6. Исследование проводилось для различного количества и заполнения исходных таблиц генератора. Рассматривались первые 256 слов каждой из последовательностей. Успешным прохождением теста является нахождение результата расчета статистики критерия ($z_в$) в пределах критических значений. Примем уровень значимости $\alpha = 0,01$. Для такого α критические значения $z_в$: $-2,576 < z_в < 2.576$.

Таблица 6

Результаты теста критерия серий

Количество исходных таблиц	$z_в$ (заполнение исходных таблиц с помощью аддитивного	$z_в$ (заполнение исходных таблиц с помощью линейного	$z_в$ (заполнение исходных таблиц с помощью квантового

	генератора)	конгруэнтного метода)	генератора случайных чисел)
2	-0,43836	-0,56361	-0,56266
3	0,688852	2,191802	-2,0657
4	0,698043	0,815126	-0,05872
5	-2,06656	0,188859	-0,68042
6	0,313115	-0,8141	-0,06262
7	-0,93934	-0,1869	1,565573
8	-1,31418	-0,1869	-0,68885

Результаты применения критерия серий подтверждают гипотезу о случайности слов на выходе комбинационного генератора для всех вариантов количества и заполнения исходных таблиц.

Выводы

Результаты проведенного в работе исследования позволяют сформулировать следующие выводы:

– для последовательностей псевдослучайных чисел, порождаемых комбинационным генератором, успешное прохождение пакета тестирования NIST наблюдается для следующих конфигураций генератора: количество исходных генераторов (таблиц перестановок) – 5 и более; заполнение исходных таблиц – аддитивный генератор, квантовый ГСЧ;

– использование линейного конгруэнтного метода для заполнения исходных таблиц перестановок комбинационного генератора не рекомендуется для задач, требующих высокого качества последовательностей псевдослучайных чисел;

– успешный результат применения непараметрических критериев, таких как критерий знаков и критерий серий, подтверждает однородность исследуемых последовательностей со случайной последовательностью чисел (критерий знаков) и случайность слов на выходе комбинационного генератора (критерий серий).

1. Кнут Д. Э. Искусство программирования. Том 2. Получисленные алгоритмы / Дональд Э. Кнут. – М.: Вильямс, 2007. – 832с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си; [пер. с англ. под ред. Семьянова П.В.]. – [2-е изд.]. – М.: Триумф, 2002. – 816 с.
3. Random Class [Электронный ресурс]. – Режим доступа: http://msdn.microsoft.com/library/system.random%28v=vs.110%29.aspx.
4. QRNG Service [Электронный ресурс] – Режим доступа: http://qrng.physik.hu-berlin.de/.
5. Лавданский А.А. Комбинационный метод формирования последовательности псевдослучайных чисел / А.А. Лавданский, Э.В. Фауре // Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014р. / ННК «ІПСА» НТУУ «КПІ». – К.: ННК «ІПСА» НТУУ «КПІ», 2014. – С. 403-404.
6. Фауре Э.В. Оценка точности воспроизведения закона распределения дискретной случайной величины при ее преобразовании / Э.В. Фауре, А.С. Береза, Е.А. Ярославская // Вісник Хмельницького національного університету. – 2012. – №5. – С. 176-182.
7. Фауре Э.В. Закон распределения дискретной случайной величины на выходе комбинационного генератора / Э.В. Фауре // Безпека інформації. – 2014. – №2. – С. 153-158. [Электронный ресурс] – Режим доступа: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/7301/8195.
8. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков – М.: КУДИЦ-ОБРАЗ, 2003. – 240с.
9. Random Number Generation and Testing [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html.
10. Смирнов Н. В. Курс теории вероятностей и математической статистики для технических приложений / Н. В. Смирнов, И. В. Дунин-Барковский – М.: Наука. Главная редакция физико-математической литературы, 1969. – 512 с.
11. Большев Л. Н. Таблицы математической статистики / Л. Н. Большев, Н. В. Смирнов – [3-е изд.] – М.: Наука. Главная редакция физико-математической литературы, 1983. – 416 с.
12. True Random Number Service [Электронный ресурс] – Режим доступа: http:// random.org/.