ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2024, том 88, № 12, с. 1951–1956

УДК 535.2

АНАЛИЗ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ СТЕПЕНИ СЛУЧАЙНОСТИ ШУМА С ПОМОЩЬЮ НЕПРЕРЫВНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ НА ПРИМЕРЕ ПОСЛЕДОВАТЕЛЬНОСТИ ЧИСЕЛ, ФОРМИРУЕМОЙ ОПТИЧЕСКИМ ГЕНЕРАТОРОМ СЛУЧАЙНОГО ШУМА

© 2024 г. М. Э. Сибгатуллин[1, 2, *], Д. А. Мавков[1], Л. Р. Гилязов[1], Н. М. Арсланов[1]

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет имени А.Н. Туполева – КАИ», Казанский квантовый центр, Казань, Россия

[2]Государственное научное бюджетное учреждение «Академия наук Республики Татарстан», Казань, Россия

**E-mail: sibmans@mail.ru*

Поступила в редакцию 15.07.2024
После доработки 19.08.2024
Принята к публикации 30.08.2024

Изучены возможности управления параметрами последовательностей случайных чисел с помощью непрерывного вейвлет-преобразования. Показано, что изменение энергии масштабов непрерывного вейвлет преобразования может увеличивать процент прохождения тестов NIST LongestRun, FFT и Runs. Возможность увеличения вероятности прохождения тестов продемонстрирована для различных размеров исследуемой экспериментальной последовательности случайных чисел.

Ключевые слова: оптический генератор случайных чисел, непрерывный вейвлет-анализ, оптимизация, повышение степени случайности

DOI: 10.31857/S0367676524120174, **EDN:** EVKPBO

ВВЕДЕНИЕ

Получение случайных чисел является важной задачей в различных областях естественных наук, математики, экономики и статистики. В основе работы аппаратных генераторов случайных чисел (ГСЧ) в качестве источника случайности лежит использование разнообразных случайных физических процессов [1,2]. Например, для получения случайной последовательности может использоваться регистрация излучения радиоактивного распада частиц [3]. Также, в качестве источника случайности используют шумы, присутствующие в электронных схемах [4], при этом регистрируется дробовый шум, возникающий из-за квантовой природы носителей тока. Разрабатываются методы генерации случайных чисел с использованием атомарных систем. В работе [5], был предложен ГСЧ, основанный на спиновом шуме паров щелочного металла, случайность которого основана на процессе квантовых флуктуаций коллективного атомного спина, известном как спиновый шум. Оптические ГСЧ используют квантовую природу фотонов для генерации случайных битов. Существует несколько схем реализации оптических ГСЧ, одной из которых является схема с детектированием состояния одиночных фотонов [6]. Еще одним подходом реализации ГСЧ в случае однофотонных событий является регистрация временных интервалов между однофотонными событиями, которые являются независимыми квантовыми случайными величинами [7]. При генерации последовательности случайных чисел на основе многофотонных процессов регистрируется интенсивность излучения, а не отдельные фотоны [8,9], что значительно увеличивает скорость генерации случайных чисел.

Одной из важных задач при генерации случайных чисел оптическими генераторами случайных чисел, основанными на квантовых принципах, является экстракция случайной битовой последовательности, которая формирует ряд истинно случайных чисел [10,11]. В работе [12] предложен подход к формированию случайных последовательностей на основе выравнивания значений мощности дискретного вейвлет-преобразования для оптимизации работы оптического ГСЧ. Полученный модифицированный ряд чисел исследовался с применением тестов NIST, используемых для оценки случайности последовательностей битов [13]. Было показано, что после применения подхода [12] происходит улучшение прохождения тестов LongestRun, FFT и Runs. При

этом, в случае LongestRun и FFT процент успешно прошедших тест последовательностей увеличивался с 7 % и 89 % до 81 % и 95 % соответственно. Однако при этом процент успешно проходящих тест Runs последовательностей составил всего лишь от 1 до 15 % в зависимости от различных комбинаций выравниваемых значений мощности. В отличие от дискретного вейвлет-преобразования, непрерывное вейвлет-преобразование [14] обеспечивает большее разрешение по частоте, что позволяет более детально анализировать и преобразовывать исследуемые сигналы. В данной работе представлены результаты эффективности применения непрерывного вейвлет-преобразования для экспериментальной последовательности случайных чисел, которая была получена ГСЧ, принцип работы которого состоит в следующем [12]. Лазерное излучение подается на вход светоделителя, разделяющего излучение на два одинаковых по мощности потока, которые детектируются на двух pin фотодиодах. Электрические сигналы такого балансного детектора вычитаются, чтобы убрать из сигнала постоянную классическую компоненту сигнала. Полученная последовательность разностного сигнала оцифровывается и используется в настоящей работе. Исследования проводились при различных значениях размеров выборки случайных чисел и количества выравниваемых масштабов вейвлет-преобразования. Было показано, что при определенных размерах выборки варьирование параметров непрерывного вейвлет-преобразования позволяет увеличить процент успешного прохождения теста Runs при сохранении процента прохождения тестов LongestRun и FFT. На основе этого, предложено определять оптимальные параметры математической обработки данных ГСЧ путем оптимизации эффективности прохождения различных тестов NIST.

МАТЕМАТИЧЕСКАЯ ОБРАБОТКА С ПРИМЕНЕНИЕМ НЕПРЕРЫВНОГО ВЕЙВЛЕТ-АНАЛИЗА

Непрерывное вейвлет-преобразование $W(a,b)$ одномерного сигнала $f(t)$ представляет собой двумерный массив, отражающий изменение вклада различных частотных компонент с течением времени:

$$W(a,b) = |a|^{1/2} \int_R f(t)\psi\left(\frac{t-b}{a}\right)dt, \qquad (1)$$

где a — масштаб, b — сдвиг, $\psi(t)$ — базисный вейвлет. По аналогии с мощностью фурье-преобразования, определяется энергия $E(a)$ непрерывного вейвлет-преобразования, которая характеризует относительный вклад вейвлет-коэффициентов на масштабах в общий сигнал:

$$E(a) = \int W^2(a,b)db \qquad (2)$$

При проведении расчетов, исходный сгенерированный сигнал разбивался на последовательности, содержащие равное количество сгенерированных чисел. Для каждой последовательности выполнялось непрерывное вейвлет-преобразование. Затем проводилось выравнивание значений энергии на масштабах, путем итерационного уменьшения вейвлет коэффициентов на выравниваемых масштабах, по следующей схеме:

$$\begin{aligned} &E(1) = E(2), \\ &E(1) = E(2) = E(3), \\ &E(1) = E(2) = E(3) = E(4) \qquad (3) \\ &... \\ &E(1) = E(2) = E(3) = E(4) = ...E(a) \end{aligned}$$

После каждого выравнивания энергий производилось обратное непрерывное вейвлет-преобразование и оценка эффективности прохождения тестов NIST новой числовой последовательности. При этом применялось два подхода выравнивания энергий: по минимуму и по среднему. При выравнивании по минимуму среди значений энергий выравниваемых масштабов определялся масштаб с минимальным значением энергии $E_{\min}(a)$, после чего вейвлет-коэффициенты всех остальных масштабов уменьшались до значения $E_{\min}(a)$. При выравнивании по среднему, определялось среднее значение энергии $E_{\text{mean}}(a)$ между выравниваемыми масштабами, после чего вейвлет-коэффициенты масштабов, у которых $E < E_{\text{mean}}(a)$ увеличивались, а для масштабов с $E > E_{\text{mean}}(a)$ — уменьшались. При этом вводится числовой параметр D, определяющий границы интервала, в который должны попасть значения энергий выравниваемых масштабов. Нижняя граница интервала определяется как $E_{\text{mean}}(a) - E_{\text{mean}}(a)D$, верхняя граница $E_{\text{mean}}(a) + E_{\text{mean}}(a)D$. Выбор параметра D определяется исходя из соотношения между временем расчетов и размеров интервала энергий, в данной работе $D = 0.5$.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Применяя предложенный алгоритм выравнивания энергий, были проведены исследования по влиянию способа выравнивания (по минимуму или по среднему) и количества выравниваемых масштабов. На рис. 1 изображены зависимости процента прохождения теста NIST от количества масштабов N, для которых проходило выравнивание энергий. При этом N меньше на единицу числа выравниваемых масштабов, то есть значение $N = 1$ означает, что выравнивались значения энергий для первого и второго масштабов $E(1) = E(2)$, $N = 2$ — для масштабов один, два и три $E(1) = E(2) = E(3)$, аналогично для всех остальных значений. Для сравнения, графики построены в одном масштабе, размер исследуемой последовательности 1000

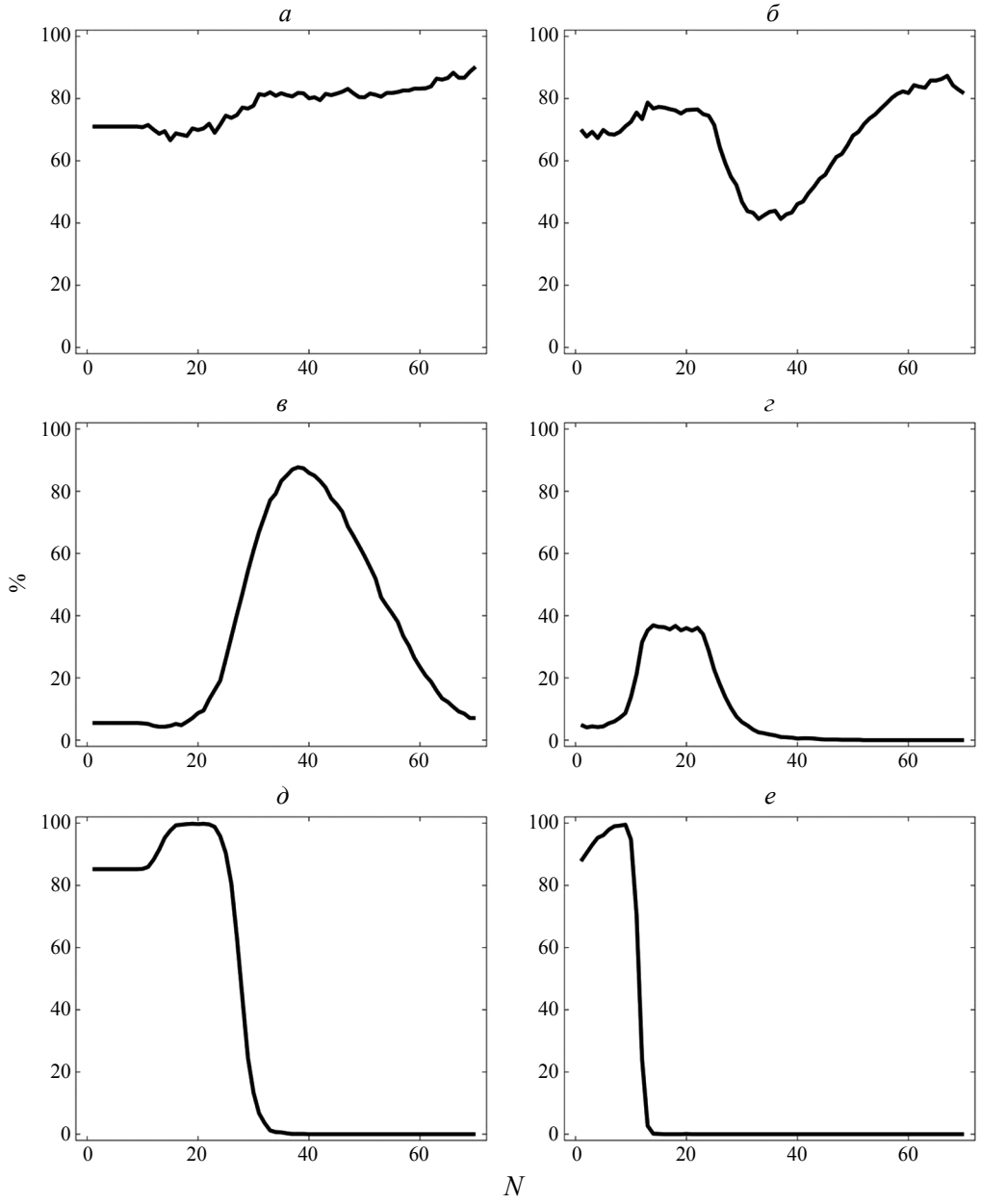

Рис. 1. Зависимость процента успешных прошедших тест NIST последовательностей в зависимости от количества масштабов непрерывного вейвлет-преобразования, для которых выполнялось выравнивание энергий: тест FFT, выравнивание по среднему (*а*); тест FFT, выравнивание по минимуму (*б*); тест LongestRun, выравнивание по среднему (*в*); тест LongestRun, выравнивание по минимуму (*г*); тест Runs, выравнивание по среднему (*д*); тест Runs, выравнивание по минимуму (*е*).

элементов Для теста FFT, выравнивание по среднему (рис. 1*а*), процент успешно прошедших последовательностей не опускается ниже 60 % при любом значении выравниваемых масштабов, достигая глобального максимума 90 % при выравнивании с 1 по 70 масштабы и локального максимума 83 % при выравнивании с 1 по 47 масштабы. В случае выравнивания по минимуму (рис. 1*б*) наблюдается локальный максимум 78 % при выравнивании 13 масштабов и глобальный максимум 87 % при выравнивании 67 масштабов. Также при этом образуется область, в которой эффективность прохождения теста опускается ниже 60 % при выравнивании по 27 масштаб и по 46 масштаб. Тест FFT нацелен на выявление равномерности распределения мощности различных частот, присутствующих в генерируемой последовательности, выявление периодических структур, которые могут указывать на предсказуемость, по сути, определяя, насколько сбалансированы вклады от высокочастотных

и низкочастотных гармоник. Таким образом, случай выравнивания по минимуму для интервала масштабов с 1 по 27, с 1 по 28, ..., с 1 по 46 для рассматриваемого оптического ГСЧ приводит к появлению периодических структур в спектре сигнала и не должен выполнятся для рассматриваемого ГСЧ. В случае выравнивания по среднему значению энергии подобных ограничений нет и возможно указывать практически любое значение выравниваемых масштабов. Тест LongestRun, выравнивание по среднему (рис. 1*в*), формирует ярко выраженный максимум 87 % при выравнивании масштабов с 1 по 38. При этом выше 60 % значения формируются в области выравнивания по 30 и по 49 масштабы. При выравнивании до 20 масштаба эффективность прохождения теста не превышает 10 %. В случае теста LongestRun и выравнивания по минимуму, эффективность прохождения теста при всех значениях выравниваемых масштабов не превышает 38 %, при этом область максимума эффективности наблюдается при значениях выравнивания с 1 по 14 и с 1 по 22 масштабы, тогда как при выравнивании по среднему значению в этих областях масштабов наблюдается минимум эффективности. Тест LongestRun тестирует последовательность чисел на то, как долго идут подряд одинаковые биты максимальной длины. Сравнивается длина самой длинной последовательности с ожидаемыми значениями для теоретической последовательности. Если значение существенно отличается от ожидаемого, это может свидетельствовать о наличии предсказуемости, что является нежелательным в криптографических приложениях. Фактически проверяется наличие существования самого длительного тренда в генерируемом сигнале, который будет являться коррелированным участком сигнала во временной области, снижая степень случайности генерируемой последовательности. Применение выравнивания по минимальному значению энергии увеличивает эффективность прохождения теста LongestRun с 7 % для исходной сгенерированной ГСЧ последовательности до 38 %, но при этом уступает в эффективности применения алгоритмов обработки с применением расчета по среднему значению для непрерывного вейвлет-анализа и дискретного вейвлет-анализа [12], которые дают сопоставимые значения эффективности в 87 % и 81 % соответственно. Тест Runs, эффективность которого не превышала 15 % при применении дискретного вейвлет преобразования [12], демонстрирует существенное увеличение эффективности выше 85 % уже при выравнивании первого и второго масштабов по среднему значению энергии (рис. 1*д*), достигая максимального значения 99 % при выравнивании в области с 1 по 16 и с 1 по 23 масштабы. Выше 60 % эффективности наблюдается при выравнивании по 27 масштаб. В случае выравнивания по минимальному значению энергии (рис. 1*г*) максимальное значение эффективности 99 % наблюдается при выравнивании до 9 масштаба, область эффективности выше 60 % формируется при выравнивании по 11 масштаб, с резким спадом до 20 % при выравнивании по 12 масштаб. Тест Runs анализирует последовательность на наличие непрерывных последовательностей одинаковых битов. Если количество таких последовательностей велико, это означает присутствие большого количества коррелированных участков в сигнале. Результаты расчетов показывают, что тест Runs существенно зависит от влияния высокочастотных компонент, точнее от их соотношения, так как высокочастотные компоненты обладают большей разницей по значениям энергии от масштаба к масштабу и выравнивание их вклада в результирующий сигнал значительно улучшает прохождение теста, а добавление в процессе выравнивания более низкочастотных масштабных компонент приводит к ухудшению результатов. Существенное улучшение по сравнению с применением дискретного вейвлет-анализа можно объяснить особенностями практической реализации расчете дискретного преобразования. На каждом этапе преобразования исследуемый сигнал проходит через высокочастотный и низкочастотный фильтры, в результате чего сигнал разделяется на низкочастотную и высокочастотную компоненты, при этом разделение происходит посередине частотного диапазона. Таким образом, для исходного сигнала с областью частот от 1 до 1000 Гц, после первого этапа выполнения дискретного преобразования, будут соответствовать два сигнала, определенных на частотных областях от 1 до 500 Гц и от 500 до 1000 Гц. После чего низкочастотная составляющая опять пропускается через фильтры высоких и низких частот, давая два сигнала с областями от 1 до 250 Гц и от 250 до 500 Гц. При этом сигналы от 500 до 1000 Гц и от 250 до 500 Гц образуют, соответственно, первый $j=1$ и второй $j=2$ масштабы дискретного вейвлет-преобразования. В отличие от дискретного, непрерывное вейвлет-преобразование разделяет исследуемый сигнал на более детальные в частотной области компоненты благодаря возможности изменять параметр масштаба $a=1,2,3,...$ с заданным дискретным шагом. В результате непрерывное вейвлет-преобразование позволяет проводить выравнивание энергий на масштабах, которые в случае дискретного преобразования все находятся на $j=1$ масштабе.

Были проведены исследования влияния размеров последовательностей, которая принимала значения 300, 500, 700 и 1000 элементов, на эффективность прохождения тестов NIST. По графикам, приведенным на рис. 1 оценивались оптимальные, с точки зрения эффективности прохождения рассматриваемыми тестами, масштабы вейвлет-преобразования для которых выполнялось выравнивание значений энергий. Результаты приведены в табл. 1. Указаны результаты расчетов для различных длин последовательностей и различных выравниваемых масштабов. Через косую черту приведены значения

для вычислений выравнивания энергий по среднему / по минимуму. Как видно из таблицы, основные изменения по эффективности прохождения тестов затрагивают три теста: FFT, LongestRun и Runs. При этом эффективность прохождения теста FFT не опускается ниже 70 % для всех рассматриваемых длин последовательностей. При длине последовательности равной 300 чисел прохождение тестов дает хорошие результаты, кроме теста Linear Complexity, который исследуемая числовая последовательность не проходит. Этот тест оценивает количество предыдущих битов, необходимых для восстановления текущего бита в последовательности с помощью линейного рекуррентного соотношения. Чем длиннее последовательность, тем большую степень случайности она может демонстрировать с точки зрения теста Linear Complexity. Это видно из табл. 1, где уже для последовательности длиной 500 элементов, после выравнивания энергий масштабов, эффективность прохождения данного теста составляет более 90 %. Также стоит отметить, что при увеличении длины исследуемой последовательности результаты прохождения тестов LongestRun и Runs демонстрируют обратную корреляцию. Например, для длины 700 элементов и при выравнивании с 1 по 29 масштаб относительно средней энергии, эффективность прохождения теста LongestRun составляет 68 %, а теста Runs — 72 %. При увеличении количества выравниваемых масштабов до 30, то есть на один масштаб, эффективность прохождения теста LongestRun вырастает до 75 %, а теста Runs падает до 57 %. Поэтому, при применении предлагаемого подхода, необходимо определиться с минимальным размером выборки, которая будет подходить для поставленных перед исследователем задач, а потом подобрать оптимальное количество масштабов, обеспечивающее удовлетворяющий, с точки зрения прохождения тестов NIST, результат.

ЗАКЛЮЧЕНИЕ

Рассмотрен подход на основе непрерывного вейвлет-анализа математической обработки сигнала, генерируемого оптическим ГСЧ, позволяющий увеличить процент прохождения тестов NIST LongestRun, FFT и Runs. Рассмотрена эффективность подхода в зависимости от размера выборки. В случае длительности последовательности генерируемых чисел до 300 элементов, рассматриваемые тесты NIST демонстрируют процент успешность прохождения тестов выше 90 %. При увеличении размеров выборки необходимо подбирать масштаб вейвлет-преобразования, относительно которого будет осуществляться выравнивание остальных значений энергии, для увеличения процента прохождения рассматриваемых тестов. Проведенные исследования необходимы при реализации аппаратного комплекса оптического ГСЧ на основе разрабатываемого нами алгоритма улучшения параметров случайных последовательностей с помощью вейвлет-преобразований на ПЛИС [15,16], что позволит избежать потерь при экстракции и увеличить скорость генерации ГСЧ

Исследование проведено при финансовой поддержке Минобрнауки России (рег. номер НИОКТР 121020400113-1).

СПИСОК ЛИТЕРАТУРЫ

1. *Herrero-Collantes M., Garcia-Escartin J.C.* // Rev. Modern Phys. 2017. V. 89. No. 1. Art. No. 015004.
2. *Mannalatha V., Mishra S., Pathak A.* // Quantum Inf. Process. 2023. V. 22. Art. No. 439.
3. *Kim T., Lee S., Yun S. et al.* // Proc. 23rd Int. Conf. WISA 2022 (Jeju Island, 2022). P. 277.
4. *Petrie C.S., Connelly J.A.* // IEEE TCAS-I. 2000. V. 47. No. 5. P. 615.

Таблица 1. Тесты NIST для различных размеров исследуемой экспериментальной последовательности случайных чисел, полученных после выравнивания энергий вейвлет-коэффициентов

Тест NIST	300	500	700	1000
	1—30/1—12	1—29/1—12	1—29/1—12	1—28/1—12
Approximate Entropy	99 / 99	99 / 99	99 / 99	99 / 99
Block Frequency	99 / 99	99 / 99	99 / 99	99 / 99
Cumulative Sums	99 / 99	99 / 99	99 / 99	99 / 99
FFT	95 / 94	89 / 87	83 / 81	74 / 75
Frequency	99 / 99	99 / 99	99 / 99	99 / 99
Linear Complexity	0 / 0	93 / 93	93 / 93	90 / 92
NonOverlapping Template	90 / 93	90 / 93	89 / 93	91 / 93
LongestRun	94 / 86	83 / 67	68 / 44	40 / 21
Runs	94 / 95	86 / 98	72 / 84	63 / 70
Serial	92 / 90	92 / 89	92 / 89	90 / 88

5. *Katsoprinakis G., Polis M., Tavernarakis A. et al.* // Phys. Rev. A. 2008. V. 77. Art. No. 054101.
6. *Argillander J., Alarcón A., Xavier G.* // J. Optics. 2022. V. 24. Art. No. 064010.
7. *Khanmohammadi A., Enne R., Hofbauer M. et al.* // IEEE Photonics J. 2015. V. 7. No. 5. P. 1.
8. *Grosshans F., Van Assche G., Wenger J. et al.* // Nature. 2003. V. 421. P. 238.
9. *Symul T., Assad S.M., Lam P.K.* // Appl. Phys. Lett. 2011. V. 98. Art. No. 231103.
10. *Балыгин К.А., Кулик С.П., Молотков С.Н.* // Письма в ЖЭТФ. 2024. Т. 119. № 7. С. 533; *Balygin K.A., Kulik S.P., Molotkov S.N.* // JETP Lett. 2024. V. 119. No. 7. P. 538.
11. *Bikos A., Nastou P., Petroudis G., Stamatiou Y.* // Criptography. 2023. V. 7. No. 4. P. 54.
12. *Сибгатуллин М.Э., Гилязов Л.Р., Мавков Д.А., Арсланов Н.М.* // Изв. РАН. Сер. физ. 2023. Т. 87. № 12. С. 1796; *Sibgatullin M.E., Gilyazov L.R., Mavkov D.A., Arslanov N.M.* // Bull. Russ. Acad. Sci. Phys. 2023. V. 87. No. 12. P. 1869.
13. *Strydom C., Soleymani S., Özdemir Ş.K., Tame M.S.* // New J. Phys. 2024. No. 26. Art. No. 043002.
14. *Евстифеев Е.В., Москаленко О.И.* // Изв. РАН. Сер. физ. 2020. Т. 84. № 2. С. 300; *Evstifeev E.V., Moskalenko O.I .*// Bull. Russ. Acad. Sci. Phys. 2020. V. 84. No. 2. P. 230.
15. *Захаров В.М., Шалагин С.В., Гумиров А.И.* // Вест. Дагестан. гос. ун-та. Сер. 1. Естеств. науки. 2023. Т. 38. № 3. С. 28.
16. *Obadi A.B., Zeghid M., Kan P.L.E.* // EEE Access. 2022. V. 10. P. 126767.

Analysis of the possibility of increasing the degree of randomness of noise using a continuous wavelet transform on the example of a sequence of numbers generated by an optical random noise generator

M. E. Sibgatullin[1,2,*], D. A. Mavkov[1], L. R. Gilyazov[1], N. M. Arslanov[1]

[1] Kazan National Research Technical University, Kazan Quantum Centre, Kazan, 420111 Russia
[2] Tatarstan Academy of Sciences, Kazan, 420111, Russia
**e-mail: sibmans@mail.ru*

The possibilities of controlling the parameters of random number sequences using a continuous wavelet transform are investigated. It is shown that changing the energy of the scales of the continuous wavelet transform can increase the percentage of passing the NIST LongestRun, FFT and Runs tests. The possibility of increasing the percentage of passing tests has been demonstrated for various sizes of the experimental sequence of random numbers under study.

Keywords: optical random number generator, continuous wavelet analysis, optimization, increasing the degree of randomness