ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2023, том 87, № 12, с. 1796–1801

УДК 535

ОПТИМИЗАЦИЯ РАБОТЫ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ InGaAs pi-n ФОТОДИОДА В ГОМОДИННОЙ СХЕМЕ С ПРИМЕНЕНИЕМ ДИСКРЕТНОГО ВЕЙВЛЕТ-АНАЛИЗА

© 2023 г. М. Э. Сибгатуллин[1, 2, 3, *], Л. Р. Гилязов[1], Д. А. Мавков[1], Н. М. Арсланов[1]

[1]*Федеральное государственное бюджетное образовательное учреждение высшего образования "Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ", Казань, Россия*

[2]*Государственное научное бюджетное учреждение "Академия наук Республики Татарстан", Казань, Россия*

[3]*Федеральное государственное автономное образовательное учреждение высшего образования "Казанский (Приволжский) федеральный университет", Казань, Россия*

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

Поступила в редакцию 24.07.2023 г.
После доработки 14.08.2023 г.
Принята к публикации 28.08.2023 г.

Предложен подход для оптимизации работы генератора случайных чисел на основе дискретного вейвлет-анализа. Показано, что управление вкладом масштабных компонент вейвлет-преобразования в сигнал может увеличить степень случайности генерируемого ряда чисел.

DOI: 10.31857/S036767652370309X, **EDN:** QJPWDP

ВВЕДЕНИЕ

Криптографические системы, использующие случайные числа, требуют оборудования, способного генерировать числа, чей случайный характер обеспечивается физическими процессами, которые невозможно предсказать и, следовательно, использовать для взлома системы шифрования [1]. Одним из классов такого оборудования являются оптические генераторы случайных чисел, которые генерируют сигналы на основе случайной регистрации фотонов [2, 3]. Однако аппаратные генераторы случайных чисел (ГСЧ) подвержены воздействию внешних факторов, таких как свойства регистрирующей аппаратуры, которые могут внести закономерности в генерируемый сигнал и, тем самым, снизить степень случайности генерируемой последовательности чисел. В связи с этим требуется проведение дополнительной обработки сигнала для оптимизации работы ГСЧ и увеличения степени случайности генерируемой последовательности чисел [4]. Коммерческие ГСЧ также дополняются программными методами постобработки генерируемых данных [5].

Нами был использован аппаратный генератор случайных чисел на основе гомодинного генератора случайного шума. Для этого было проведено разностное детектирование сигналов на выходах оптического светоделителя, что привело к формированию шума. Случайные свойства полученного шума были оценены с помощью тестов NIST [6]. Однако было выявлено, что генерируемая случайная последовательность не проходит некоторые тесты и требуется применение дополнительных процедур для оптимизации работы ГСЧ и увеличения степени случайности шума.

Предложен подход, основанный на разложении генерируемого сигнала на масштабные компоненты с применением дискретного вейвлет-анализа, и исследовании свойств каждой масштабной компоненты как отдельного сигнала [7]. В отличие от фурье-анализа, вейвлет-анализ позволяет проводить исследование одномерного сигнала одновременно во временной и частотной областях, что позволяет получить более полную информацию о свойствах исследуемой последовательности. Это может значительно улучшить степень случайности генерируемой последовательности чисел.

Предложен подход, основанный на изменении вклада некоторых масштабных компонент в суммарный генерируемый сигнал. В результате обработки степень случайности генерируемой последовательности чисел улучшается, что отражается в более эффективном прохождении трех тестов NIST. При этом не наблюдается потери эффективности прохождения остальных тестов. Этот позволяет оптимизировать работу генератора случайных чисел и повысить уровень безопасности криптографических систем, использующих такой генератор.

ГЕНЕРАЦИЯ СЛУЧАЙНОГО ШУМА

В традиционном методе оптической генерации случайных чисел применяется светоделитель в оптической схеме и регистрация однофотонных импульсов с помощью фотодетекторов [8, 9]. В данной работе для этой цели был использован лазер с распределенной обратной связью, работающий на длине волны 1550 нм и с шириной полосы 1 МГц, и с мощностью излучения 20 мВт. Излучение направлялось на вход волоконного Y-разветвителя 50/50, а его выходы подключались к фотоприемникам гомодинного детектора. Фотоприемники состояли из двух балансно включенных InGaAs pi-n фотодиодов, производства ООО “Лазерском”, с частотой среза 2 ГГц, низким темновым током 0.03 нА и емкостью порядка 0.65 пА. Такая оптическая схема позволяет генерировать случайные числа с высокой степенью случайности и является эффективным средством для создания криптографических систем.

Сигнал с фотодиодов усиливался операционным усилителем Texas Instruments OPA847 в режиме трансимпедансного усиления. Затем проходил через фильтр верхних частот (ФВЧ), который удалял шум с частотами ниже 95 МГц, и дополнительно усиливался операционным усилителем Analog Devices AD8099 с коэффициентом усиления 20. Затем выходной сигнал проходил через фильтр нижних частот (ФНЧ) с частотой среза около 105 МГц и подключался к 50 Ом СВЧ коннектору. В результате использования данной оптической схемы была сгенерирована последовательность случайных чисел, размер выборки которой составил один миллион элементов. На рис. 1. приведена гистограмма экспериментального шума. Черным цветом (сплошная линия) показана аппроксимация гистограммы гауссовым распределением со следующими параметрами: интенсивность $I = 41253$ отн. ед., полуширина $\delta = 0.43$ отн. ед., положение максимума $\omega_0 = 0$ отн. ед., среднеквадратичное отклонение гистограммы от аппроксимации $\sigma = 0.39$. Сгенерированный шум в используемой оптической схеме имеет отчетливые выбросы на определенных значениях гистограммы, что объясняется тем, что сигнал не подвергался процедуре фильтрации паразитных аппаратных шумов, которая улучшила бы его степень случайности.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Были проведены тесты NIST для оценки степени случайности сгенерированной последовательности. Исследуемая выборка разбивалась на непересекающиеся подпоследовательности длиной 1000 элементов, оценивался процент подпоследовательностей, успешно прошедших тесты (табл. 1).

В результате, более 89 процентов подпоследовательностей прошли восемь тестов. Однако

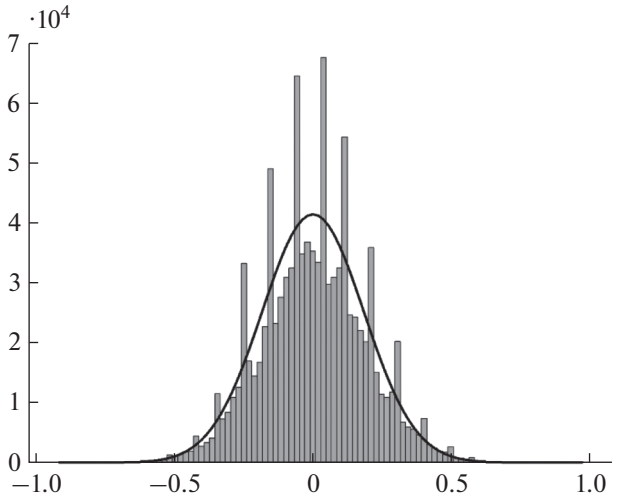

Рис. 1. Гистограмма экспериментального шума.

только 7 процентов подпоследовательностей прошло тест LongestRun. Тест NIST LongestRun является одним из наиболее требовательных к генераторам случайных чисел, поэтому его прохождение является важным показателем качества генерации случайных чисел. Подобный результат является следствием наличия пиков значений в гистограмме на рис. 1, что приводит к большим сериям одинаковых значений в последовательностях. Таким образом, необходимо определить некоторую процедуру эффективного устранения серий близких значений.

Для анализа и увеличения степени случайности генерируемого шума в данной работе предложено применить вейвлет-анализ. Дискретный вейвлет-анализ является эффективным инструментом для проведения процедуры денойзинга (удаления шума) путем изменения вейвлет-коэффициентов на определенных масштабах в зависимости от параметров сигнала и выполнении обратного вейвлет-преобразования [10, 11]. Дискретное вейвлет-преобразование сигнала f может быть представлено как линейное преобразование:

$$w = Wf, \tag{1}$$

Таблица 1. Тесты NIST экспериментального шума

Тест NIST	Результат
Approximate Entropy	100
Block Frequency	100
Cumulative Sums	100
FFT	89
Frequency	100
Linear Complexity	92
NonOverlapping Template	100
LongestRun	7
Serial	92

Таблица 2. Показатель Херста масштабных компонент экспериментального шума

Масштаб	1	2	3	4	5	6	7	8	9
Показатель Херста	0.16 ± 0.08	0.17 ± 0.08	0.24 ± 0.06	0.43 ± 0.08	0.59 ± 0.09	0.75 ± 0.11	0.91 ± 0.08	0.99 ± 0.03	0.99 ± 0.01

где $w = [d_{1,1},\ldots d_{1,w1}, d_{2,1},\ldots d_{2,w2}, a_{J,1},\ldots a_{J,wJ}]$ содержит детальные вейвлет-коэффициенты d на масштабах $j = 1,\ldots J$ и аппроксимационные вейвлет-коэффициенты a на масштабе J. Элементы матрицы $W = W(N, J, h_n)$, представляющие собой дискретное вейвлет-преобразование, определяются из пирамидального алгоритма Маллата [12]. На рис. 2*а* показан генерируемый шум и его разложение на масштабные компоненты с применением дискретного вейвлет-анализа (рис. 2*б*).

Можно рассматривать генерируемую последовательность как набор сигналов, обладающих различными частотными свойствами – масштаб 1 содержит высокочастотную компоненту, по мере возрастания масштаба происходит увеличение низкочастотной составляющей в сигнале.

Одной из количественных характеристик позволяющих провести классификацию случайных шумов относительно частотного состава, является показатель Херста H: 1) низкочастотный шум ($1/2 < H < 1$), характеризуется долговременными корреляциями (персистентность); 2) высокочастотный шум (антиперсистентность) ($0 < H < 1/2$) [13]. В табл. 2 приведен расчет показателя Херста для масштабных компонент экспериментального шума. Приведены средние значения для тысячи подпоследовательностей на каждом масштабе.

Как видно из табл. 1 масштабы с 1 по 3 характеризуются низкими значениями показателя Херста и, соответственно, высокочастотной структурой. Масштабы с 5 по 8 характеризуются высокими значениями показателя Херста и обладают низкочастотной структурой. Показатель Херста на масштабе 4 может принимать значения как больше, так и меньше 0.5 (в пределах доверительного интервала). При этом показатель Херста пятого масштаба не опускается ниже значения 0.5, а показатель Херста на третьего масштаба не превышает значения 0.5. Таким образом, четвертый масштаб можно рассматривать в качестве границы, между низкочастотными (персистентными) и высокочастотными (антиперсистентными) масштабными компонентами.

Для количественного описания вклада различных масштабных компонент с сигнал применяют мощность $P(j)$ дискретного вейвлет-преобразования:

$$P(j) = \sum_k d_{j,k}^2, \qquad (2)$$

где $d_{j,k}$ – детальные вейвлет-коэффициенты. На рис. 3*а* показано распределение мощности дискретного вейвлет-преобразования для экспериментального шума. Наибольшее значение мощности имеют масштабы с 1 по 3, начиная с 4 масштаба значения мощности выравниваются.

На рис. 3*б* приведено значение приращения величины показателя Херста ΔH между масштабными компонентами. Величина ΔH растет с увеличением масштаба и достигает максимума для приращения между четвертым и третьим масштабами. После этого приращение показателя Херста начинает уменьшаться.

Таким образом, значение показателя Херста, мощность дискретного вейвлет-преобразования, приращение показателя Херста между масштабами показывают, что четвертый масштаб является своеобразным “граничным” масштабом, который разделяет шумы с различной структурой.

Для коррекции генерируемого шума нами предложена итерационная схема по уменьшению вейвлет-коэффициентов на определенных масштабах:

$$\varphi^{(i+1)} = W^{-1}\theta W\varphi^{(i)},\ \ \varphi^{(0)} = f,\ \ \varphi^{(1)} = W^{-1}\theta W\varphi^{(0)},$$
$$\varphi^{(i)} = W^{-1}\theta W\varphi^{(i-1)},\ldots i = 0,1,2,\ldots, \qquad (3)$$

где в качестве первого приближения используется экспериментальный сигнал f, W – дискретное вейвлет-преобразование, W^{-1} – обратное дискретное вейвлет-преобразование, θ – коэффициент, который либо увеличивает ($\theta > 0$), либо уменьшает ($\theta < 0$) вейвлет-коэффициенты на выбранном масштабе.

Сравнивая значения показателя Херста для различных масштабов (табл. 2) и распределения мощности вейвлет-преобразования по масштабам (рис. 3*а*) можно обратить внимание, что высокочастотные компоненты, находящиеся на масштабах 1-3, имеют сильно перекрывающиеся значения показателя Херста (с учетом доверительного интервала) и, в то же время, сильно различаются по величине мощности вейвлет-преобразования. В то время, как масштабы с низкочастотными компонентами близки друг к другу по величине мощности. Было предложено провести процедуру выравнивания значений мощности на масштабах с первого по третий, чтобы выровнять значения мощности высокочастотных компонент аналогично распределению мощности для низкочастотных компонент. Выполнялось итерационное уменьшение значений вейвлет-коэффициентов на первом и втором масштабах. Критерием прерывания итераций яв-

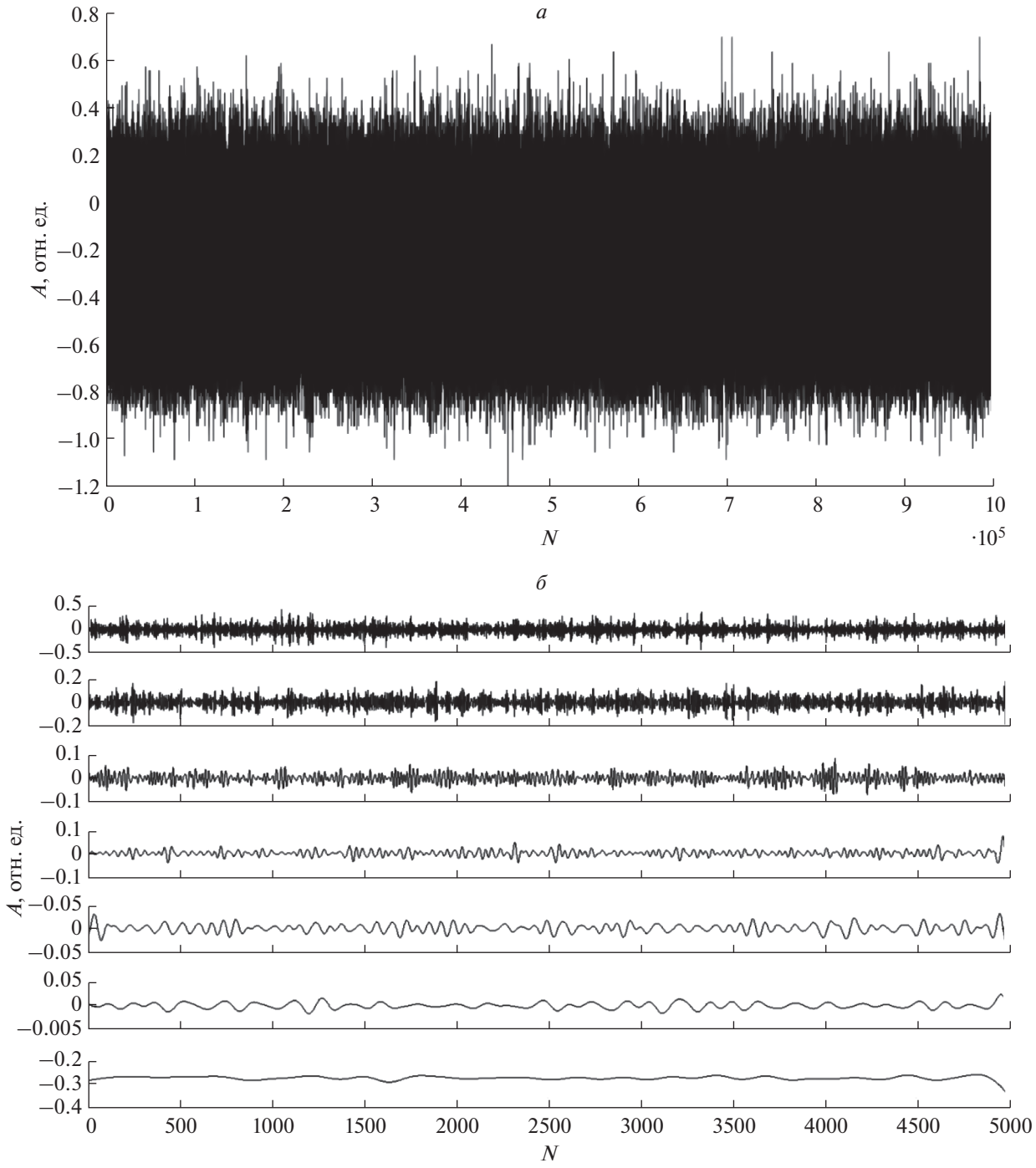

Рис. 2. Экспериментальный шум (*а*); масштабные компоненты шума (*б*).

лялось равенство значений мощности первого и второго масштабов значению мощности третьего масштаба. Затем выполнялось обратное вейвлет-преобразования для получения сигнала.

В табл. 3. приведены результаты проведения тестов NIST для сигналов, полученных путем различных комбинаций выравнивания мощности дискретного вейвлет-преобразования: (1-3) – выравнивание мощности с первого по третий масштаб; (1-4) – выравнивание мощности с первого по четвертый масштаб; (1-3-4-11) – выравнивались отдельно масштабы с первого по третий и отдельно с четвертого по одиннадцатый масштаб; (1-11) – выравнивание мощности с первого по одиннадцатый масштаб.

Наилучшие результаты получены при реализации схем (1-3) и (1-3-4-11). При реализации схемы (1-3) процент успешного прохождения теста

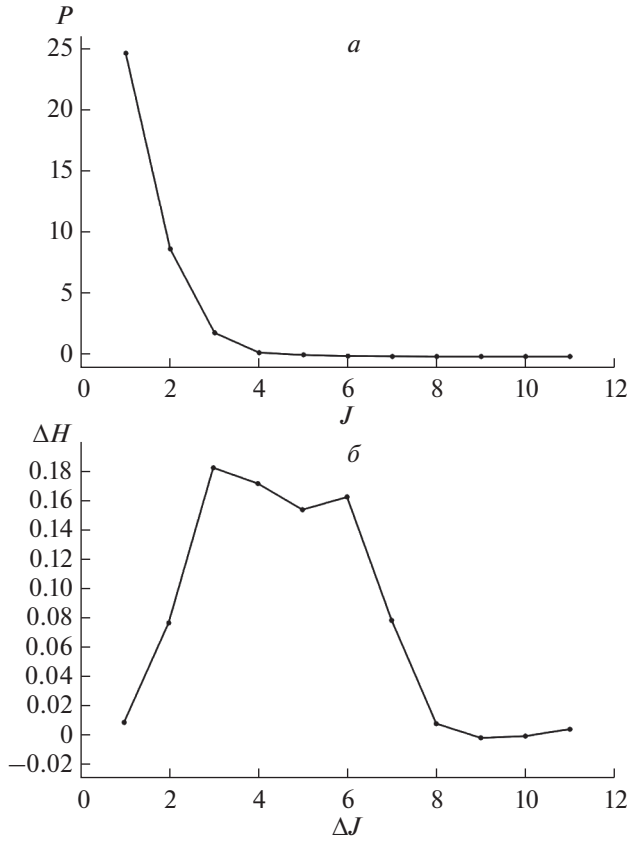

Рис. 3. Зависимость мощности вейвлет-преобразования от масштаба для экспериментального шума (*а*); зависимость приращения показателя Херста от масштаба для экспериментального шума (*б*).

“FFT” увеличивается на 6%, теста “LongestRun” на 74%, теста “Runs” на 1%, при этом процент успешного прохождения оставшихся тестов не изменяется. В случае применения схемы (1-3-4-11) происходит увеличение до 15% успешного прохождения теста “Runs”, однако при этом ухудшается процент успешного прохождения практически всех тестов, хотя он и остается выше 50%. В случае выравнивания к одному значению мощности вейвлет-коэффициентов на всех одиннадцати масштабах наблюдается существенное ухудшение процентов успешного прохождения практически всех тестов. Обусловлено это тем, что при выравнивании мощности всех масштабов, вклад низкочастотных компонент начинает быть сопоставим с вкладом высокочастотных компонент, а это означает появление в последовательности низкочастотных трендов, что существенно ухудшает свойства генерируемой последовательности. Анализ результатов тестирования в случае выравнивания (1-4) показывает ухудшения процента прохождения тестов NIST. Это подтверждает, что на четвертом масштабе существуют низкочастотные компоненты, которые при росте их относительного вклада в сигнал ухудшают его с точки зрения случайного характера последовательности. Предложенный алгоритм обратим, путем математических преобразований возможно получить исходную сгенерированную ГСЧ числовую последовательность. Однако это возможно только при том условии, что до выполнения обратного преобразования имеются точные данные о распределении мощности вейвлет-преобразования по масштабам исходной последовательности, а это означает, что известна сама исходная последовательность. Без этой информации обратное преобразование теряет смысл, так как будет получено бесконечное множество числовых последовательностей, выбрать истинную из которых невозможно.

На рис. 4 приведена гистограмма шума после проведенной математической обработки с применением дискретного вейвлет-анализа (выравнивание мощности масштабов 1-3) и черным цветом показана аппроксимация функцией гаусса, со следующими параметрами: $I = 42600$ отн. ед., $\delta = 0.2$ отн. ед., $\omega_0 = 0$ отн. ед., $\sigma = 0.02$.

После применения математической обработки по выравниванию мощности на первом, втором и третьем масштабах, среднеквадратичное отклонение между аппроксимирующей функции и гистограммой уменьшается в 20 раз по сравнению среднеквадратичным отклонением аппроксимирующей функции от гистограммы в случае необработанного сгенерированного шума. Также про-

Таблица 3. Тесты NIST для различных комбинаций выравнивания мощности вейвлет-преобразования

Тест NIST	1-3	1-4	1-3-4-11	1-11
Approximate Entropy	100	100	100	100
Block Frequency	100	81	93	0
Cumulative Sums	100	99	79	2
FFT	95	76	84	92
Frequency	100	100	77	9
Linear Complexity	92	90	93	90
NonOverlapping Template	100	100	100	100
LongestRun	81	12	54	0
Runs	1	0	15	0
Serial	92	82	93	0

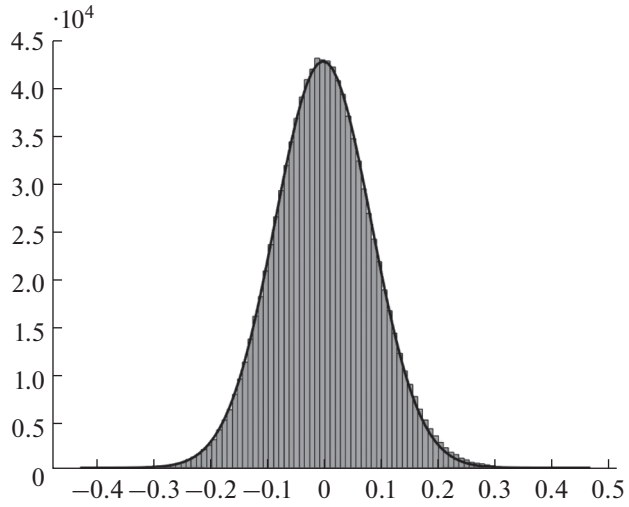

Рис. 4. Гистограмма шума после выравнивания масштабных компонент 1, 2, 3 по мощности вейвлет-преобразования.

падают выбросы в гистограмме, распределение становится приближенным к гауссовому.

ЗАКЛЮЧЕНИЕ

Проведено исследование свойств случайного шума, полученного с применением оптического генератора случайных чисел на основе InGaAs pi-n фотодиода в гомодинной схеме. Предложено для анализа сгенерированной числовой последовательности применить дискретный вейвлет-анализ и расчет числовых характеристик для каждой масштабной компоненты.

Применение дискретного вейвлет-анализа позволило провести разделение сгенерированного шума на группы масштабных компонент с низкочастотной и высокочастотной структурами. Предложена итерационная процедура, которая выравнивает значение мощности на различных масштабах вейвлет-преобразования. Показано, что необходимо выравнивать мощности высокочастотных компонент, не затрагивая низкочастотные. Предлагаемый подход показал высокую эффективность, улучшились результаты прохождения тестов NIST, гистограмма распределения стала гауссовой, пропали локальные выбросы на гистограмме.

Научные исследования проведены при финансовой поддержке Минобрнауки России (рег. номер НИОКТР 121020400113-1).

СПИСОК ЛИТЕРАТУРЫ

1. *Petura O.* True random number generators for cryptography: Design, securing and evaluation. PhD thesis. Universite de Lyon, 2019. 145 p.
2. *Балыгин К.А., Зайцев В.И., Климов А.Н. и др.* // ЖЭТФ. 2018. Т. 153. № 6. С. 879; *Balygin K.A., Zaitsev V.I., Klimov A.N. et al.* // JETP. 2018. V. 126. No. 6. P. 728.
3. *Петров В.М., Шамрай А.В., Ильичев И.В. и др.* // Фотоника. 2021. Т. 15. № 1. С. 70; *Petrov V.M., Shamray A.V., Ilyichev I.V. et al.* // Photonics. Russ. 2021. V. 15. No. 1. P. 70.
4. *Пикуза М.О.* // Докл. БГУИР. 2022. Т. 20. № 7. С. 43.
5. *Jacak M., Jóźwiak P., Niemczuk J, Jacak J.* // Sci. Reports. 2021. V. 11. Art. No. 16108.
6. *Bassham L., Rukhin A., Soto J. et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg: National Institute of Standards and Technology, 2010. 131 p.
7. *Павлов А.В.* // в кн.: Квантовые и оптические методы обработки информации и вычислений. Т. 1. Санкт-Петербург: Университет ИТМО, 2021. С. 90.
8. *Ma X., Yuan X., Cao Z. et al.* // Quant. Inform. 2016. No. 2. Art. No. 16021.
9. *Jennewein T., Achleitner U., Weihs G. et al.* // Rev. Sci. Instrum. 2000. No. 71. P. 1675.
10. *Московский С.Б., Сергеев А.Н., Сидорова Е.И., Марудов А.А.* // Вестн. МИФИ. 2021. Т. 10. № 1. С. 77.
11. *Kralj L., Lenasi H.* // Front Physiol. 2022. No. 13. Art. No. 1076445.
12. *Mallat S.* A wavelet tour of signal processing. N.Y.: Academic Press, 1999. 240 p.
13. *Chandrasekaran S., Poomalai S., Saminathan B. et al.* // Meteorol. Appl. 2019. V. 26. No. 3. P. 511.

Optimization of the random number generator based on InGaAs pi-n photodiode in a homodyne scheme using discrete wavelet analysis

M. E. Sibgatullin[a, b, c, *], L. R. Gilyazov[a], D. A. Mavkov[a], N. M. Arslanov[a]

[a] *Kazan National Research Technical University, Kazan, 420111 Russia*
[b] *Academy of Sciences of the Republic of Tatarstan, Kazan, 420111 Russia*
[c] *Kazan (Volga Region) Federal University, Kazan, 420008 Russia*
**e-mail: sibmans@mail.ru*

An approach is proposed to optimize the operation of a random number generator based on discrete wavelet analysis. It is shown that controlling the contribution of the scale components of the wavelet transform to the signal can increase the degree of randomness of the generated series of numbers.

Keywords: random number generator, discrete wavelet analysis, Hurst exponent, entropy