

Научная статья

DOI 10.66424/2071-8217-2026-3-2

УДК 519.248:004.056.5

МЕТОД ОЦЕНКИ КАЧЕСТВА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ РАСЧЕТА СПЕКТРАЛЬНОЙ ЭНТРОПИИ

А. В. Касьянов^{1,2*}, А. Ю. Гришенцев³¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия²ООО «Специальный Технологический Центр» (ООО «СТЦ»), Санкт-Петербург, Россия³Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия

✉ *kasjanov@inbox.ru

ДЛЯ ЦИТИРОВАНИЯ

Касьянов А. В., Гришенцев А. Ю.
Метод оценки качества генераторов случайных чисел на основе расчета спектральной энтропии // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 25–48.
DOI: 10.66424/2071-8217-2026-3-2

ПОСТУПИЛА 30.04.2026**ПРИНЯТА** 15.05.2026**ОПУБЛИКОВАНА** 13.10.2026

© Касьянов А. В., Гришенцев А. Ю.

Издатель: Санкт-Петербургский политехнический университет Петра Великого

АННОТАЦИЯ

Целью исследования являлись разработка и математическое обоснование метода оценки качества случайности выходных последовательностей генераторов (псевдо-) случайных чисел на основе спектральной энтропии. Для решения частных задач использовались следующие методы: дискретное преобразование Фурье для расчета спектра сигналов; непараметрический бутстреп для построения эмпирических распределений оценок и определения порогов принятия решения; метрика Махаланобиса для количественного сравнения исследуемых реализаций с эталонной областью и формализации критерия принадлежности к классу случайных последовательностей. На тестовом примере детерминированной последовательности натуральных чисел установлено, что энтропия Шеннона может давать ложноположительное заключение о случайности, тогда как спектральная энтропия устойчиво выявляет неслучайность. Исследование случайных последовательностей, полученных с помощью физического генератора в различных режимах работы, позволило сделать вывод, что метод спектральной энтропии выявляет деградацию случайности последовательностей при неверно выбранных режимах работы генератора. Следует отметить, что предлагаемый метод спектральной энтропии по эффективности решаемой задачи не уступает стандартным тестам NIST STS, а в некоторых случаях превосходит их. В рамках проведенных испытаний установлено, что синтезируемые последовательности на основе поточного алгоритма шифрования ChaCha20 удовлетворяет критерию случайности полученного с помощью метода спектральной энтропии, что интерпретируется как соответствие требованиям, предъявляемым к криптографическим источникам случайности. Исследования показали, что разработанный метод позволяет детектировать неслучайность последовательностей, полученных с помощью регистров сдвига с линейной обратной связью. Научная новизна: теоретически обоснован и разработан на уровне готовности к практическому применению метод оценки качества генераторов (псевдо-)случайных чисел на основе вычисления спектральной энтропии. Установлено, что метод обладает повышенной устойчивостью оценки качества случайности по сравнению с энтропией Шеннона. Практическая значимость заключается в повышении эффективности оценивания качества случайных и псевдослучайных последовательностей.

КЛЮЧЕВЫЕ СЛОВА

Случайность, битовая последовательность, спектральная энтропия, спектральная плотность мощности, метод бутстреп, статистическое тестирование, расстояние (метрика) Махаланобиса, межквартильный размах, регистры сдвига с линейной обратной связью

Original article

DOI 10.66424/2071-8217-2026-3-2

METHOD OF EVALUATING THE QUALITY OF RANDOM-NUMBER GENERATORS BASED ON SPECTRAL ENTROPY CALCULATION

A. V. Kasyanov^{1,2*}, A. Yu. Grishencev³¹Saint Petersburg Electrotechnical University, St. Petersburg, Russia²Special Technology Center LLC (STC LLC), St. Petersburg, Russia³ITMO University, St. Petersburg, Russia✉ *kasjanov@inbox.ru

FOR CITATION

Kasyanov A. V., Grishencev A. Yu.
Method of evaluating the quality of
random-number generators based on
spectral entropy calculation.

Problems of information security.
Computer systems.

2026. No. 3, pp. 25–48.

DOI: 10.66424/2071-8217-2026-3-2
(In Russian)

RECEIVED 30.04.2026**ACCEPTED** 15.05.2026**PUBLICATION** 13.10.2026

ABSTRACT

The aim of this study was to develop and mathematically substantiate a method for assessing the randomness quality of output sequences produced by random and pseudorandom number generators based on spectral entropy. To solve the individual subproblems, the following methods were used: the discrete Fourier transform for signal spectrum computation; nonparametric bootstrap for constructing empirical distributions of estimates and determining decision thresholds; and the Mahalanobis distance for quantitative comparison of the analyzed realizations with a reference region and for formalizing the criterion of membership in the class of random sequences. Using a test case based on a deterministic sequence of natural numbers, it was established that Shannon entropy may yield a false-positive conclusion of randomness, whereas spectral entropy reliably detects non-randomness. The study of random sequences generated by a physical generator under different operating modes made it possible to conclude that the spectral entropy method detects degradation of sequence randomness when the generator operating conditions are chosen incorrectly. It should be noted that, in terms of effectiveness for the problem under consideration, the proposed spectral entropy method is not inferior to the standard NIST STS tests and, in some cases, outperforms them. Within the conducted experiments, it was established that the synthesized sequences generated using the ChaCha20 stream cipher satisfy the randomness criterion obtained by the spectral entropy method, which is interpreted as compliance with the requirements imposed on cryptographic sources of randomness. The study also showed that the developed method makes it possible to detect non-randomness in sequences generated by linear feedback shift registers (LFSRs). The scientific novelty of the work lies in the fact that a method for evaluating the quality of random and pseudorandom number generators based on spectral entropy computation has been theoretically substantiated and developed to a level of readiness for practical application. It has been established that, compared with Shannon entropy, the method provides greater robustness in randomness quality assessment. The practical significance lies in improving the efficiency of assessing the quality of random and pseudorandom sequences.

KEYWORDS

Randomness, bit sequence, spectral entropy, power spectral density, bootstrap method, statistical testing, Mahalanobis distance (metric), interquartile range, linear feedback shift registers

1. ВВЕДЕНИЕ

Надежность современных криптографических механизмов в значительной мере определяется эффективностью генераторов случайных и псевдослучайных чисел (Г(П)СЧ), поскольку именно они формируют случайные криптографические ключи, определяют параметры цифровых подписей и иные конфиденциальные данные [1–3], от которых зависит устойчивость алгоритмов шифрования и механизмов аутентификации [4]. Для систем защиты каналов широкополосной связи данное утверждение также справедливо, поскольку метод синтеза алфавитов ортогональных широкополосных сигнальных символов основан на генерации псевдослучайных n -мерных векторов [5, 6]. Идеальная модель работы генератора предполагает, что его выходной сигнал должен быть эквивалентен серии независимых испытаний «честной» монеты, при этом каждый бит формируется без зависимости от остальных, получение 0 или 1 равновероятны [7]. Однако в реальных условиях источники энтропии подвержены проявлению программных и аппаратных дефектов, в том числе умышленных модификаций.

Показателем качества случайных данных является энтропия битовой последовательности. Согласно Клоду Элвуду Шеннону, энтропия характеризует уровень неопределенности и непредсказуемости случайной величины [8–10], а в контексте криптографической безопасности отражает резерв секретности, предоставляемый источником случайности. Анализ энтропии выходных последовательностей, генерируемых Г(П)СЧ, позволяет formalизовать предъявляемые к генераторам критерии непредсказуемости и вычислительной неотличимости от истинно случайных источников, что является обязательным условием для функционирования средств криптографической защиты информации. При этом недостаточная энтропия или наличие статистических зависимостей может привести к уменьшению эффективного пространства ключей

и значительному увеличению вероятности успешного проведения криптоанализа, что в критических случаях способно привести к полной компрометации системы. Международные и национальные стандарты, а также методические рекомендации, в том числе документы NIST SP 800-90B [11] и BSI AIS-20/31 [12], акцентируют внимание на том, что первичным объектом анализа является энтропия источника, а не исключительно результаты статистического тестирования выходного сигнала. В указанных источниках подчеркивается необходимость моделирования стохастической природы источника шума, проведения теоретического и экспериментального анализа уровня энтропии, а также установления нижних границ для средней и минимальной энтропии выходных битов. Проведение подобного анализа является необходимым как для обоснования безопасности криптографических алгоритмов, так и для соответствия регуляторным требованиям и стандартам отраслевого уровня, что особенно актуально для информационных систем, работающих с конфиденциальными данными.

Исторический опыт свидетельствует, что недостаточное внимание к анализу энтропии или ее некорректная оценка уже становились причиной значимых инцидентов в области информационной безопасности. Примером тому служат обнаруженные дефекты работы Г(П)СЧ в реализации протоколов Netscape SSL в 1996 г. [13], выявленная уязвимость в реализации OpenSSL для платформы Debian в 2008 г. [14], комплекс проблем, связанных с алгоритмом Dual_EC_DRBG [15], выявленная в 2015 г. уязвимость генератора ANSI X9.31 RNG, взлом ГПСЧ xorshift128 и MT19937 в 2021 [16, 17], а также критическая уязвимость CVE-2023-39910 в библиотеке Libbitcoin Explorer версии 3.x [18], связанная со слабостью генерации энтропии при создании приватных ключей. Последняя уязвимость привела к инциденту Milk Sad в 2023 г., когда восстановлено более 900000 приватных ключей Bitcoin с прямыми финансовыми потерями свыше 0,8 млн дол. США. Эти случаи демонстрируют, что даже

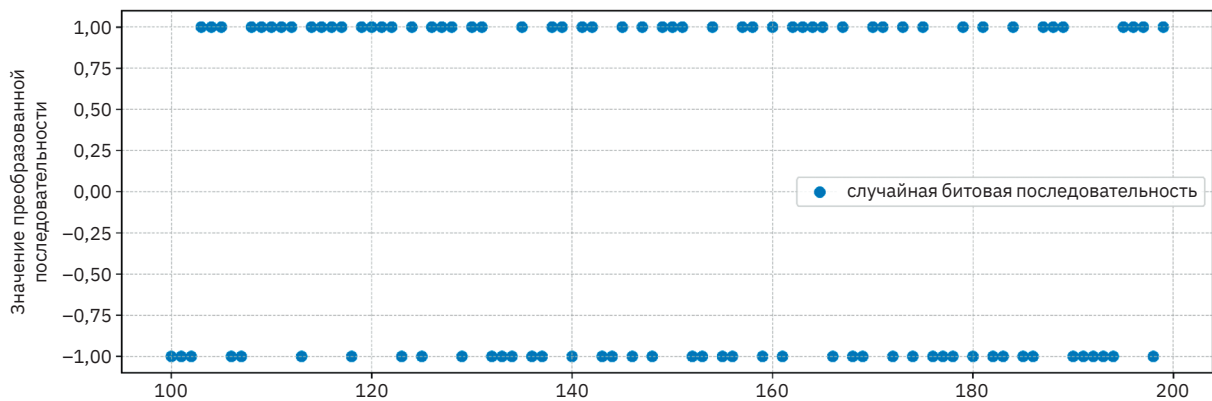


Рис. 1 | Часть преобразованной случайной битовой последовательности

Fig. 1 | Part of a transformed random bit sequence

конструкции, разработанные с соблюдением формальных требований и стандартизированные, могут оказаться практически уязвимыми при недостаточном уровне случайности или наличии предсказуемых закономерностей в выходных данных.

Таким образом, расчет и обоснование энтропии случайных битовых последовательностей является актуальной задачей, решение которой способствует повышению криптографической стойкости реализуемых протоколов и систем на основе случайных последовательностей.

Целью исследования является разработка метода оценки энтропии случайных битовых последовательностей на основе анализа спектральной плотности мощности.

2. СПЕКТРАЛЬНАЯ ЭНТРОПИЯ

Пусть $E = \{e[n]\}$, $n = \overline{0, N-1}$ – реализация битовой случайной последовательности длины N [7]. Преобразуем последовательность E к последовательности $x = \{x[n]\}$, $n = \overline{0, N-1}$ вида $\{1, -1\}$, где значения $x[i]$ формируются по правилу $x[i] = 2e[i] - 1$, пример преобразованной последовательности представлен на рис. 1.

Запишем автокорреляционную функцию для случайной битовой последовательности:

$$R_x[n] = \frac{1}{N} \sum_{i=0}^{N-1-n} x[i]x[i+n], \quad n = 0, 1, \dots, N-1, \quad (1)$$

$$R_x[n] \xrightarrow{N \rightarrow \infty} \delta_{n0}, \quad \delta_{n0} = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases}$$

где δ_{n0} – дискретная дельта-функция Кронекера.

Согласно теореме Винера – Хинчина (1934) [19], спектральная плотность мощности и автокорреляционная функция связаны между собой преобразованием Фурье. И в соответствии с предложенным в [20] алгоритмом вычисления автокорреляционной функции на основе быстрых преобразований Фурье с использованием формул Рэлея [21] и (1) получим:

$$S[k] = X[k] \times X^*[k] = F\{R_x[n]\}F, \quad (2)$$

где $S[k]$ – спектральная плотность мощности битовой последовательности; $X[k] = F\{x[n]\} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n]e^{-\frac{2\pi j}{N}kn}$ – прямое преобразование Фурье; $X^*[k]$ – величина комплексно сопряженная к $X[k]$.

Нормируем $S[k]$:

$$\frac{1}{\sum_{l=0}^{N-1} S[l]} S[k] = \bar{S}[k], \quad (3)$$

где $\bar{S}$ – нормированная спектральная плотность мощности, тогда

$$\begin{cases} 0 \leq \bar{S}[k] \leq 1, & k = \overline{0, N-1} \\ \sum_{k=0}^{N-1} \bar{S}[k] = 1 \end{cases} \quad (4)$$

Физический смысл $\bar{S}[k]$ состоит в том, что она характеризует распределение мощности сигнала по частотному спектру, т.е. $\bar{S}[k]$ можно трактовать как вероятность присутствия спектральной компоненты на частоте, соответствующей k -му частотному отсчету, для случайного битового сигнала [22]. Тогда, согласно [23], спектральная энтропия H^{SE} случайной битовой последовательности рассчитывается по формуле

$$H^{SE} = - \sum_{k=0}^{N-1} \bar{S}[k] \log_2 \bar{S}[k]. \quad (5)$$

3. РЕШАЮЩЕЕ ПРАВИЛО И МЕТРИКА ОЦЕНКИ

Для оценки соответствия исследуемого генератора криптографическим требованиям разработан метод, включающий определение метрического показателя и формулирование правила для принятия решения. Предлагаемый подход позволяет установить: генерирует ли источник данные с ожидаемым уровнем энтропии.

Для формирования критериев принятия решений (решающих правил) и идентификации метрик целесообразно использовать метод бутстреп [24] – вычислительный метод непараметрической статистики, предназначенный для приближенной оценки распределения выборочной статистики (среднего, медианы, эксцесса и т.д.) по единственной доступной реализации данных. Бутстреп основан на многократной генерации псевдовыборок посредством случайного отбора наблюдений с возвращением из исходной выборки и последующим вычислением интересующей статистики на каждой псевдовыборке.

Эмпирическое распределение исходной (эталонной) выборки рассматривается как приближение неизвестного распреде-

ления генеральной совокупности [25], что позволяет моделировать вариативность оценок методом бутстреп. Для построения реализации «эталонного» криптографического генератора использовались следующие реализации:

1. Выборка, синтезированная с использованием криптографического генератора случайных чисел, реализованного на основе системной функции `os.urandom` (Python), использующей встроенный аппаратный генератор платформы Windows и алгоритм блочного шифрования AES, при объеме выборки 400 последовательностей длиной 10^6 бит.

2. Выборка, сформированная с помощью криптографического генератора, функционирующего на основе алгоритма «Кузнечик»¹ в режиме гаммирования с обратной связью по выходу (OFB²), с использованием рекомендованных последовательностей в качестве начального вектора (IV), объем которой составляет 300 последовательностей длиной 10^6 бит.

3. Выборка, полученная при применении криптографического генератора, основанного на алгоритме «Кузнечик» в режиме гаммирования (CTR²), с использованием рекомендованных последовательностей в роли начального вектора объемом 300 последовательностей длиной 10^6 бит.

Таким образом, эталонная выборка состояла из 1000 последовательностей длиной 10^6 бит каждая (рис. 2). Длины битовых последовательностей выбраны в соответствии с рекомендациями для корректного применения асимптотических

¹ ГОСТ Р 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. № 1061-ст.

² ГОСТ Р 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. № 1062-ст.

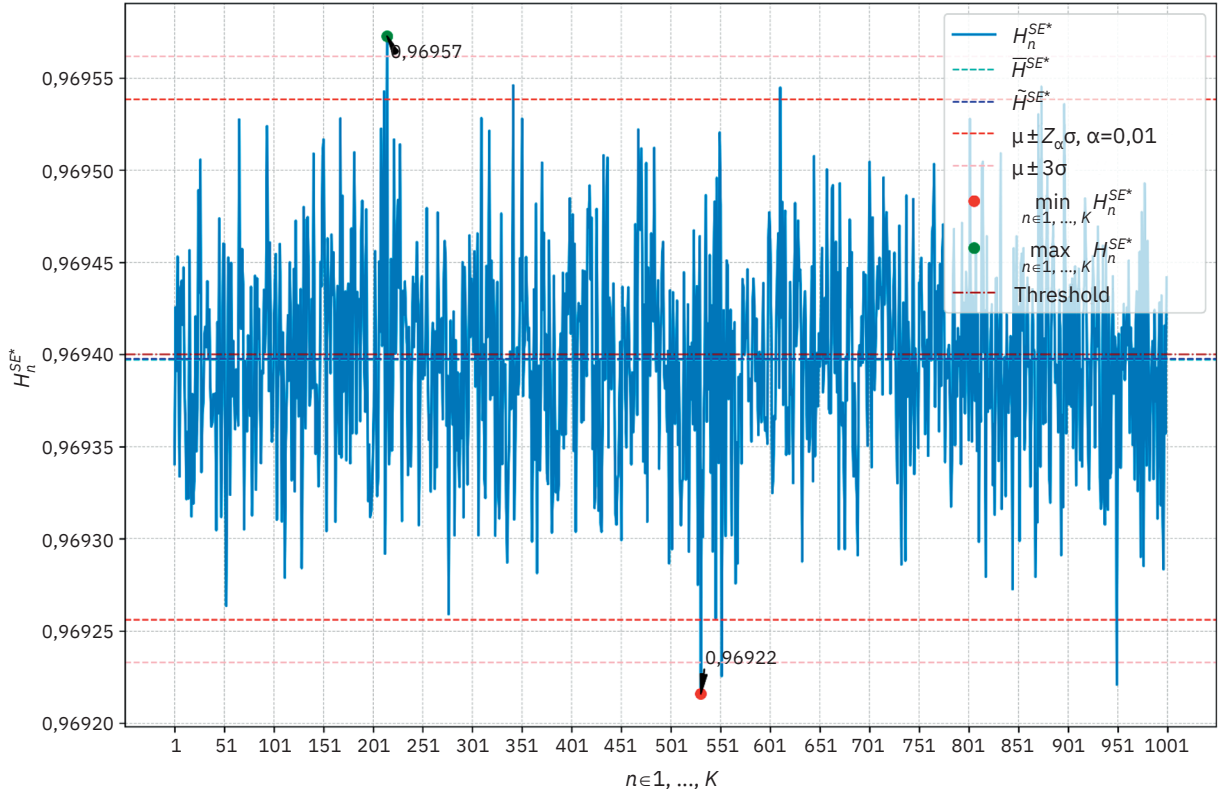


Рис. 2 | Пример визуализации эталонной выборки

Fig. 2 | Example of visualization of a reference sample

статистических тестов на случайность для оценки качества генераторов, используемых в криптографических протоколах и приложениях, для уровня значимости $\alpha=0,01$ [26]. Распределение последовательностей между тремя реализациями проводилось по долям 40, 30 и 30 %, что обеспечило репрезентативность статистических наблюдений и достаточную вариативность данных.

Имеется эталонная выборка из $K=1000$ «истинно» случайных последовательностей длины 10^6 бит. Для каждой последовательности вычисляется спектральная энтропия H_n^{SE*} , $n \in \{1, \dots, K\}$ (5). Далее калибруем область принятия решения так, чтобы она соответствовала протоколу тестирования генератора, и выполняем бутстреп моделирование.

Вычислительные этапы калибровки области принятия решения. 1. Для $b=1, \dots, B$ (где $B=10^6$ – число повторов) случайно выбираем $M=100$ значений (так как для уровня значимости $\alpha=0,01$ при

тестировании необходимо не менее 100 последовательностей [7]) из $\{H_n^{SE*}\}_{j=1}^K$ с последующим возвращением в исходную выборку.

2. Для выбранных M значений вычисляем пару статистик $\bar{H}^b, \tilde{H}^b$ и строим множество точек $\mathbf{y}^b$:

$$\begin{cases} \mathbf{y}^b = (\bar{H}^b, \tilde{H}^b) \\ \bar{H}^b = \frac{1}{M} \sum_{i=1}^M \bar{H}_i^b \\ \tilde{H}^b = \text{median}(\tilde{H}_1^b, \tilde{H}_2^b, \dots, \tilde{H}_M^b) \end{cases} \quad (6)$$

3. По множеству точек $\{\mathbf{y}^b\}_{b=1}^B$ оцениваем центральную точку μ и ковариационную матрицу Σ :

$$\mu = \frac{1}{B} \sum_{b=1}^B \mathbf{y}^b, \quad \Sigma = \text{Cov}(\mathbf{y}^1, \dots, \mathbf{y}^B), \quad (7)$$

а также строим доверительные интервал по перцентилям эмпирического распре-

деления бутстреп-оценок (среднего и медианы):

$$\overline{CI} = \left[\bar{H}_{\alpha/2}^*, +\infty \right), \quad \widetilde{CI} = \left[\tilde{H}_{\alpha/2}^*, +\infty \right), \quad (8)$$

где $\bar{H}_{\alpha/2}^*$ – $\alpha/2$ -квантиль распределения $\bar{H}^b$ бутстреп-оценок среднего; $\tilde{H}_{\alpha/2}^*$ – $\alpha/2$ -квантиль распределения $\tilde{H}^b$ бутстреп-оценок медианы.

4. Эллипс принятия решения (для уровня значимости $\alpha = 0,01$). Для каждой точки $\mathbf{y}$ определяем расстояние Махаланобиса [27, 28] по формуле

$$T(\mathbf{y}) = (\mathbf{y} - \boldsymbol{\mu})^T \Sigma^{-1} (\mathbf{y} - \boldsymbol{\mu}), \quad (9)$$

для точек $\mathbf{y}^b$ вычисляем расстояние по формуле (9)

$$T^b = T(\mathbf{y}^b) \quad (10)$$

и задаем порог C как квантиль уровня $1 - \alpha$:

$$C = \left(T^1, \dots, T^B \right)_{1-\alpha}. \quad (11)$$

Тогда 99 % эллипс принятия решения задается множеством H (по построению 99 % эталонных реализаций попадает внутрь области H):

$$H = \{ \mathbf{y} : T(\mathbf{y}) \leq C \}. \quad (12)$$

Протокол проведения тестирования генератора. Для анализа энтропийных характеристик генератора из генеральной совокупности формируется битовая выборка длиной 10^8 бит, которая далее без перекрытия способом естественного упорядочивания разбивается на $M = 100$ последовательностей длиной 10^6 бит взятых друг за другом из исходной выборки.

Для каждой последовательности, согласно (5), рассчитывается значение спектральной энтропии H_i^{obs} , $i = 1, \dots, M$.

Далее вычисляем наблюдаемую точку $\mathbf{y}^{obs}$:

$$\begin{cases} \mathbf{y}^{obs} = (\bar{H}^{obs}, \tilde{H}^{obs}) \\ \bar{H}^{obs} = \frac{1}{M} \sum_{i=1}^M H_i^{obs} \\ \tilde{H}^{obs} = \text{median}(H_1^{obs}, H_2^{obs}, \dots, H_M^{obs}) \end{cases} \quad (13)$$

Проверяем попадает ли наблюдаемая точка $\mathbf{y}^{obs}$ внутрь области H , т.е. проверяем выполнимость условия (12):

$$\mathbf{y}^{obs} \in H \Leftrightarrow T(\mathbf{y}^{obs}) \leq C. \quad (14)$$

Решающее правило. Рассмотрим формализацию решающего правила в рамках описанного протокола проведения тестирования для двоичных последовательностей длиной n бит и выбранной статистики теста $\mathbf{y}^{obs}$. Вводится два альтернативных исхода: H_0 – генератор «не отличим» от идеального источника по выбранной статистике $\mathbf{y}^{obs} = (\bar{H}^{obs}, \tilde{H}^{obs})$, при заданной схеме эксперимента ($M = 100$, $N = 10^6$ бит); H_1 – генератор статистически детектируем по выбранной статистике (т.е. дает не типичную точку в пространстве).

Если $T(\mathbf{y}^{obs}) \leq C$, то генератор согласуется с эталонной случайной моделью, при уровне значимости $\alpha = 0,01$, H_0 не отвергается и делается вывод о пригодности генератора для использования в криптографических приложениях.

Если $T(\mathbf{y}^{obs}) > C$, то проверяется условие попадания наблюдаемой точки в область пространства $\Psi = [\overline{CI}, \widetilde{CI}]$ в соответствии с (8).

Если $\mathbf{y}^{obs} \in \Psi$, то генератор не согласуется с эталонной случайной моделью при уровне значимости $\alpha = 0,01$, гипотеза H_0 отвергается, делается предположение о том, что генератор возможно пригоден (может сохранять пригодность для некоторых практических сценариев) для использования в криптографических приложениях, но необходимо дополнительное исследование.

Если $\mathbf{y}^{obs} \notin \Psi$, то гипотеза H_0 отвергается и делается вывод о том, что генератор не пригоден для использования в криптографических приложениях.

После применения основного критерия согласия осуществляется дополнительная верификация на уровне отдельных реализаций, входящих в выборку, для исключения локальных дефектов генерации, которые могли бы компенсироваться в усредненных статистических показателях. В рамках данного этапа подтверждается, что все значения спектральных

энтропий H_i^{obs} последовательностей длиной 10^6 бит взятых из выборки исследуемого генератора лежат в допустимом интервале (рис. 3):

$$H_i^{obs} \in [\mu_B - z_\alpha \sigma_B, \mu_B + z_\alpha \sigma_B], \quad (15)$$

где μ_B , σ_B – выборочное среднее и стандартное отклонение выборки; z_α – квантиль стандартного нормального распределения для уровня значимости α .

Параллельно проводится робастный контроль выбросов (рис. 4) на основе межквартильного размаха (IQR) [29], при котором значения спектральных энтропий H_i^{obs} не должны выходить за границы:

$$[Q_1 - 1,5IQR, Q_3 + 1,5IQR], \quad (16)$$

где Q_1, Q_3 – первый и третий квартили, а $IQR = Q_3 - Q_1$.

Тем самым обеспечивается, что при сохранении согласия по агрегированным характеристикам (среднему и медиане)

каждая отдельная последовательность демонстрирует спектральную энтропию H_i^{obs} , совместимую с ожидаемой вариативностью, и в выборке отсутствуют экстремальные отклонения, указывающие на аномальные реализации или эпизодические сбои в механизме генерации (т.е. проверяется однородность качества генерации по реализациям и отсутствие единичных аномалий).

При интерпретации выбросов применяется асимметричное правило: выбросы, смещенные в сторону повышенной энтропии (аномально большие значения $H_i^{obs} > \mu_B + z_\alpha \sigma_B$, максимально приближенные к теоретически максимальной энтропии) рассматриваются как не влияющие на свойства случайности по данному показателю и, следовательно, исключаются из последующих расчетов, поскольку считаются неинформативными для оценки деградации качества. Напротив, выбросы в сторону пониженной энтропии

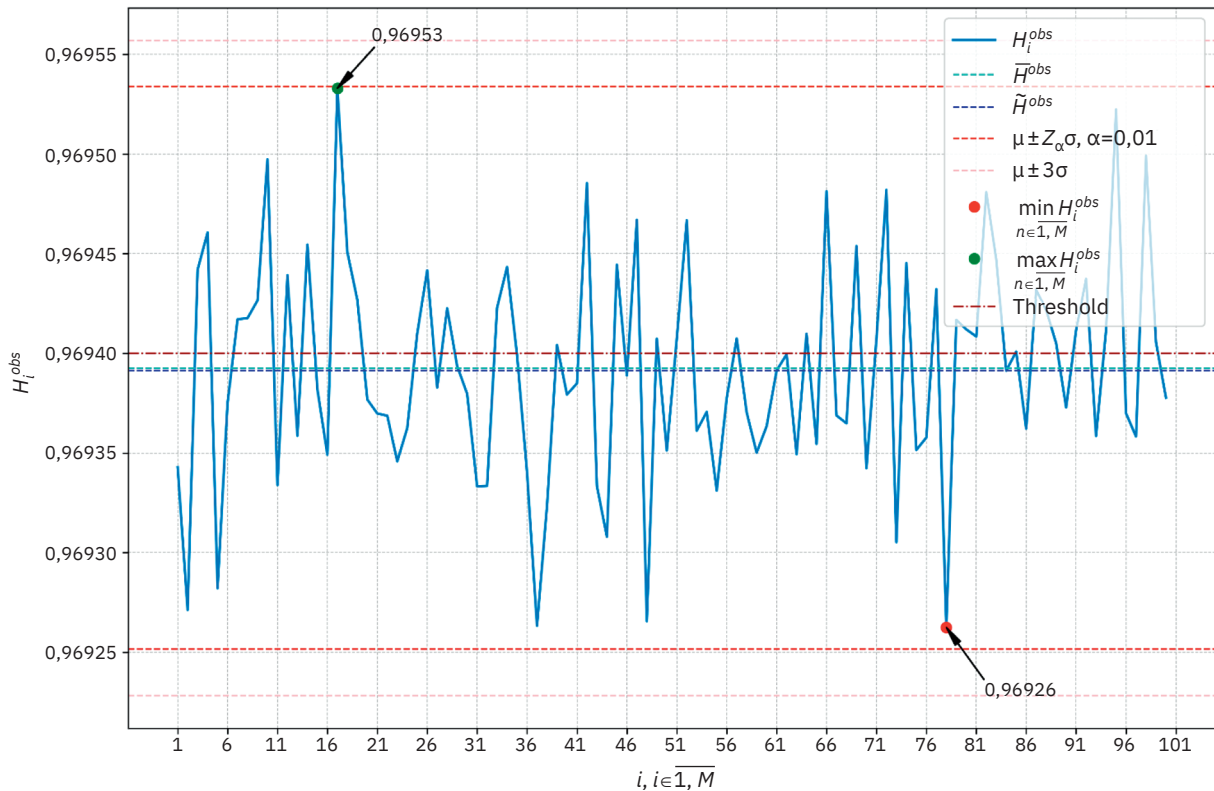


Рис. 3 | Спектральная энтропия и статистические характеристики выборки

Fig. 3 | Spectral entropy and statistical characteristics of the sample

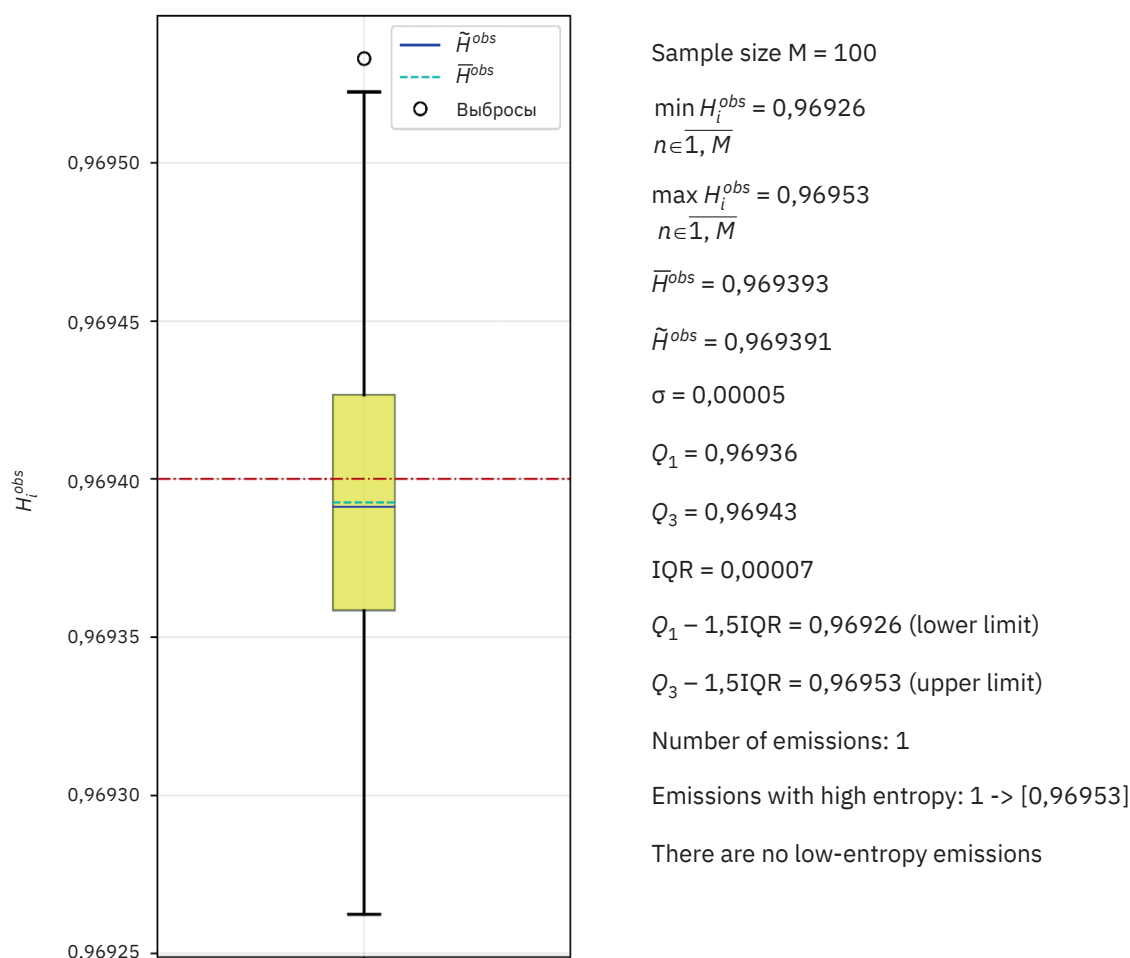


Рис. 4 | IQR и статистические характеристики выборки

Fig. 4 | IQR and statistical sample characteristics

(аномально низкие значения H_i^{obs}) интерпретируются как потенциальный признак эпизодического ухудшения свойств случайности, поэтому при их наличии генератор направляется на дополнительную проверку с использованием расширенного набора тестов. Аномальные снижения энтропии служат основным индикатором необходимости проведения дальнейших проверок для оценки стабильности работы генератора.

Проводимые проверки нацелены на установление устойчивости режима работы исследуемого генератора. Иными словами, подтверждается не только согласие агрегированных показателей генератора с идеализированным источником, но и воспроизводимость качества по ка-

ждой отдельной реализации (значения для всех последовательностей выборки остаются в пределах допустимой вариабельности).

4. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

Предложенным методом выполнено тестирование физического генератора случайных чисел, сертифицированного регулятором, и работающего в двух режимах функционирования. В первом режиме рабочая точка на вольт-амперной характеристике шумового диода выбрана вне области лавинного пробоя, что не обеспечивало оптимальные условия работы

схемы. Во втором режиме рабочая точка установлена в области лавинного пробоя. Сопоставление результатов, полученных разработанным методом, проводилось со стандартным набором статистических тестов NIST [30]. Для выполнения анализа сформированы битовые выборки длиной 10^8 бит каждая, которые далее без перекрытия, методом естественного упорядочивания, разделены на $M = 100$ последовательностей длиной 10^6 бит, извлекаемых по порядку из исходных выборок.

Представленные на рис. 5, 6 результаты указывают на более высокую диагностическую чувствительность предлагаемого подхода по сравнению со стандартным набором статистических тестов NIST применительно к задаче контроля корректности физического режима формирования случайности. В обоих режимах рабо-

ты генератора сформированные выборки удовлетворили критериям NIST, что означает отсутствие выявляемых указанными тестами статистических отклонений на уровне распределений и типовых корреляционных структур в пределах рассматриваемых длин последовательностей. Однако в первом режиме генератор эксплуатировался при заведомо нештатных условиях, вследствие чего в цифровом потоке возрастала вероятность спектральных искажений, появления доминирующих частотных компонент и снижения эффективной размерности источника энтропии.

При таких условиях выборка формально проходит NIST, что указывает на ограниченную способность стандартных статистических критериев NIST выступать индикатором физической деградации

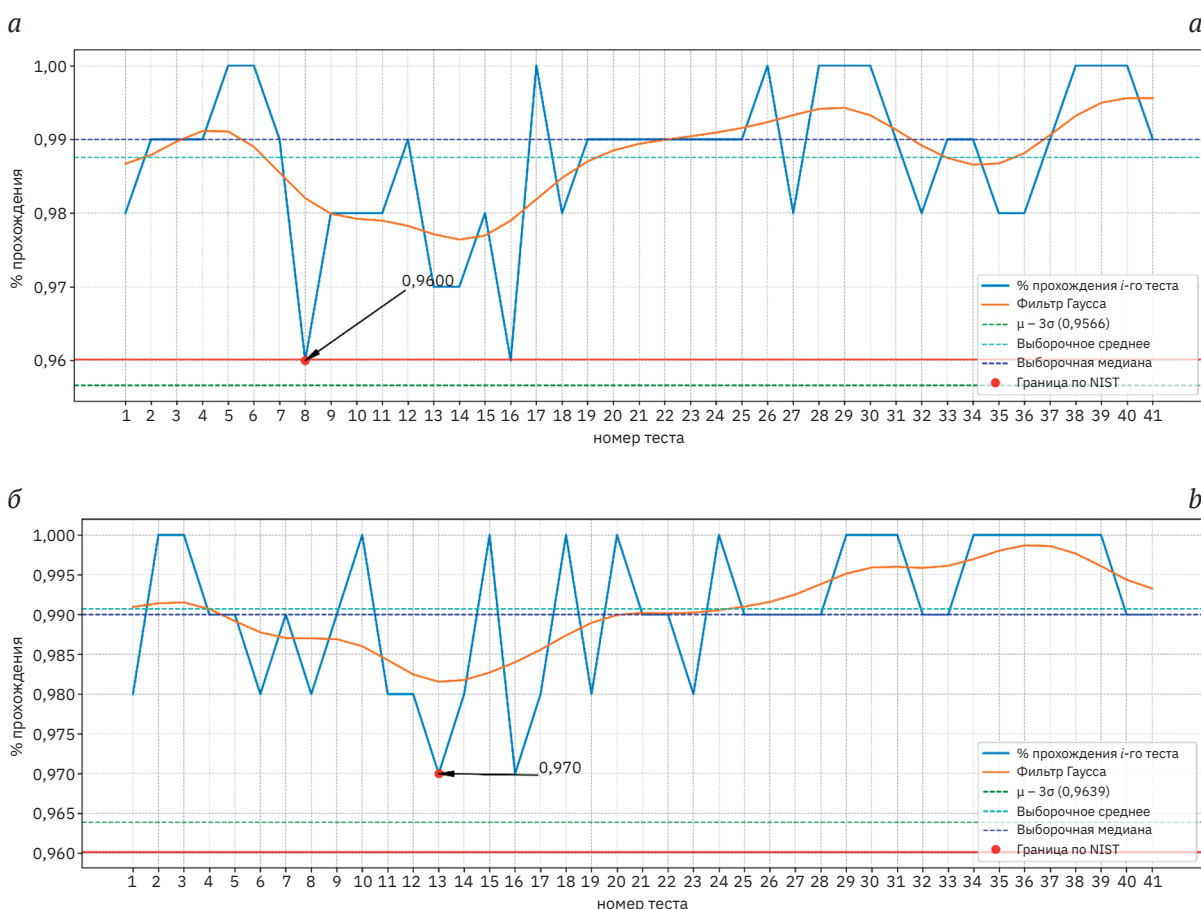


Рис. 5 | Прохождение генератором статистических тестов STS NIST в режимах 1 (а) и 2 (б)

Fig. 5 | Run STS NIST statistical tests by the generator in modes 1 (a) and 2 (b)

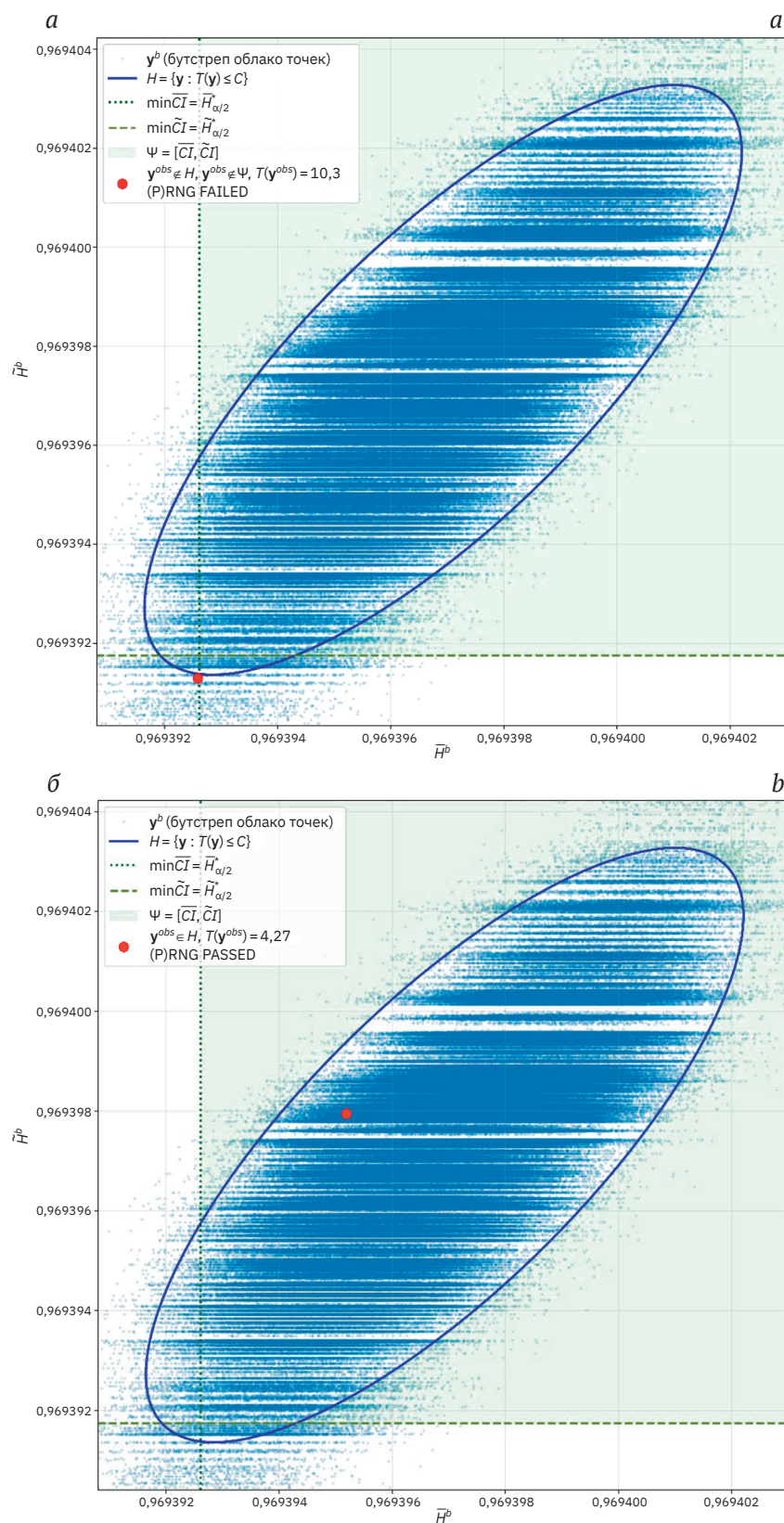


Рис. 6 | Пример применения метода спектральной энтропии для исследования физического генератора:
 а – с плохо выбранной рабочей точкой (режим 1); б – с правильно выбранной рабочей точкой (режим 2)

Fig. 6 | Example of a spectral entropy method for the study of a physical generator:
 а – with an incorrectly selected work point (mode 1); б – with the correct selected work point (mode 2)

источника энтропии. Напротив, метод спектральной энтропии является более адекватным инструментом для выявления нарушений, связанных с изменением спектрального содержания шумового сигнала.

Для первого режима включения генератора снижение спектральной энтропии и непрохождение критерия свидетельствуют о концентрации спектра и уменьшении степени «равномерности» частотного заполнения, что физически согласуется с работой диода вне лавинного пробоя. Во втором режиме, при корректной установке рабочей точки, спектральная энтропия возрастает до значений, соответствующих широкополосному шумовому процессу, и выборка проходит проверку. Таким образом, предлагаемый метод обеспечивает различение режимов, которые с точки зрения физики источника принципиально различны по качеству формирования энтропии.

Выполнено тестирование генератора псевдослучайных чисел, основанного на алгоритме ChaCha20 [31]. Указанный генератор интегрирован в OpenBSD начиная с версии 5.4 в качестве замены алгоритму RC4, а также внедрен в NetBSD начиная с версии 7.0. В ядре Linux, начиная с версии 4.8, данный генератор применяется вместо алгоритма SHA-1. Считается надежным и безопасным для применения в криптографических приложениях [32].

По результатам обработки сформированных последовательностей установлено, что исследуемый генератор успешно проходит как тестирование по методике NIST (рис. 7), так и проверку в рамках предложенного метода (рис. 8), что согласуется с его ожидаемыми статистическими характеристиками и заявленной криптографической стойкостью.

На основе регистра сдвига с линейной обратной связью [33], заданным неприводимым многочленом $f_{64} \in \mathbb{F}_2[x]$ ($\mathbb{F}_2[x]$ – кольцо многочленов над полем $\mathbb{F}_2$ из двух элементов $\{0,1\}$) степени 64 $f_{64} = x^{64} + x^{46} + x^4 + x + 1$, при начальном заполнении регистра 0ха294d3d7487098b5 сформирована

битовая выборка объема 10^8 бит. Далее выборка без перекрытия, методом естественного упорядочивания, разделена на последовательности длиной 10^6 бит. По результатам оценивания энтропия Шеннона, вычисленная по частотам битовых слов, составила $H \approx 0,9999997$, что формально соответствует почти «идеальной» случайности и демонстрирует низкую диагностическую способность данного показателя для детектирования линейной структуры регистра сдвига с линейной обратной связью. В то же время тестирование набором NIST STS показало прохождение всех тестов, за исключением теста на линейную сложность (ни одна из последовательностей не прошла этот тест), что является основанием рассматривать данный генератор как непригодный для криптографических применений. Предложенный метод на основе спектральной энтропии также классифицировал рассматриваемую последовательность как не удовлетворяющую критерию пригодности для криптографических приложений, так как точка исследуемого генератора расположилась вне области принятия решения (рис. 9).

Предлагаемый метод не уступает тестам NIST по способности выявлять линейно-детерминированные источники с большим периодом, превосходит энтропию Шеннона по чувствительности к скрытой регулярности, а для регистра сдвига с линейной обратной связью с малыми периодами обеспечивает их оперативное отсеечение за счет выраженных спектральных артефактов, проявляющихся уже на коротких фрагментах данных.

Проведен сравнительный анализ значений спектральной энтропии и энтропии Шеннона на различной длине битового слова для натурального ряда $1...2^{20}$, изначально каждое число ряда представимо в 20-битной форме. Полученные зависимости показывают принципиальное различие информативности указанных характеристик в задаче выявления неслучайной структуры. Энтропия Шеннона во всем диапазоне длин слова остается практически постоянной и близкой

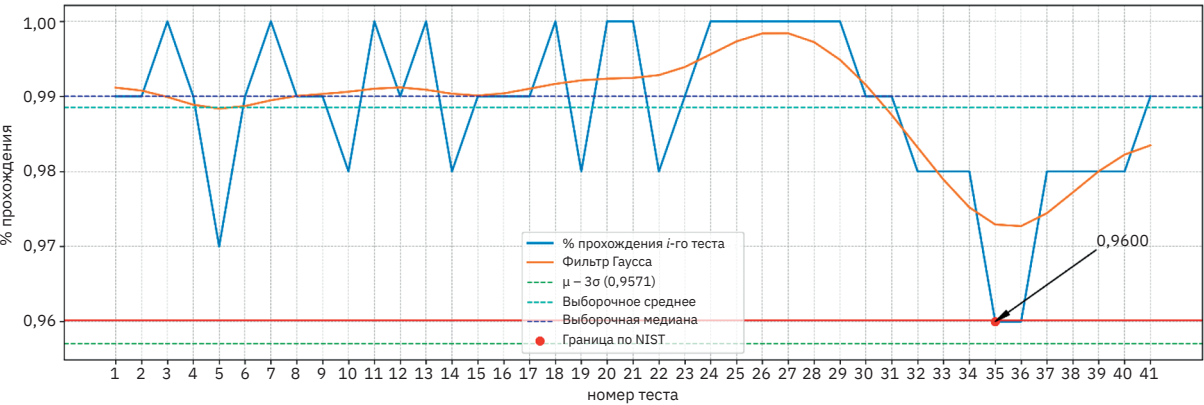


Рис. 7 | Прохождение ChaCha20 статистических тестов STS NIST

Fig. 7 | ChaCha20 STS NIST statistical tests

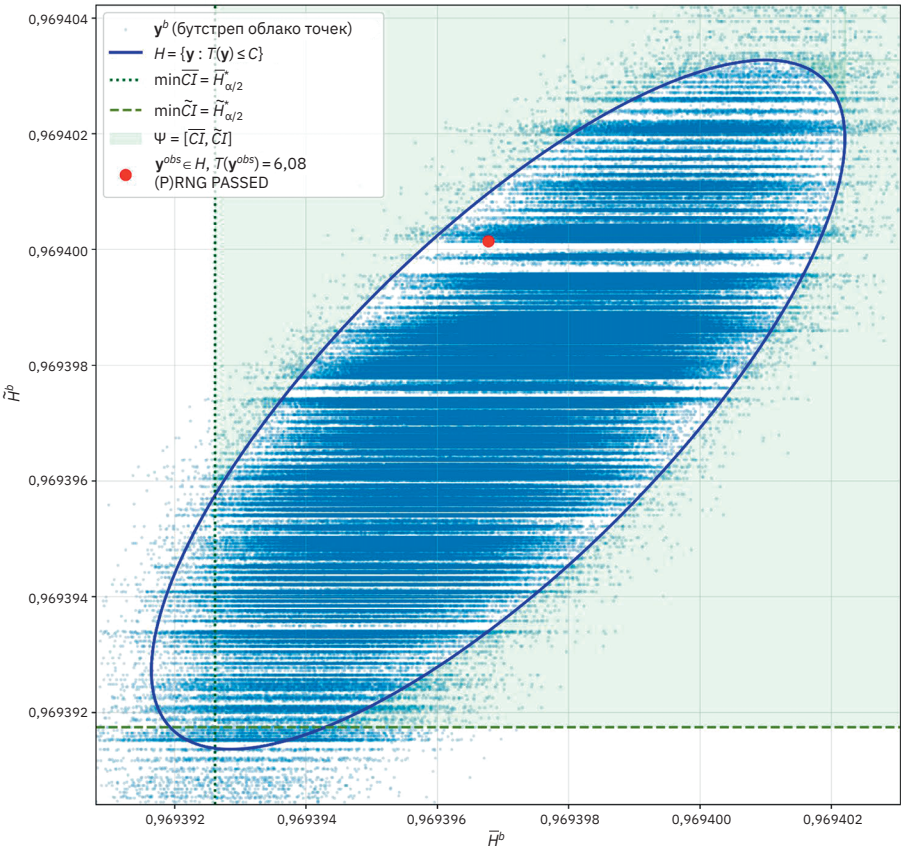


Рис. 8 | Пример применения разработанного метода к ГПСЧ

Fig. 8 | Example of application of the developed method to PRNG

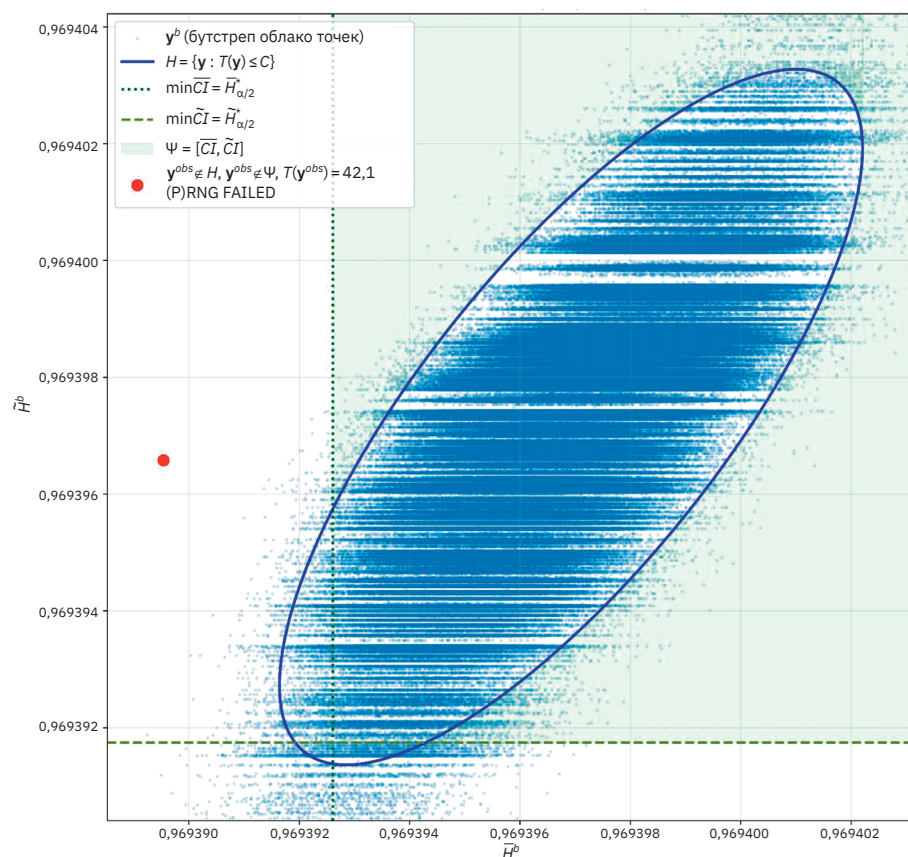


Рис. 9 | Пример применения разработанного метода к регистру сдвига с линейной обратной связью с большим периодом ($f(x)=x^{64}+x^{46}+x^4+x+1$ начальное заполнение 0xa294d3d7487098b5)

Fig. 9 | An example of applying the developed method to a large-period linear feedback shift register ($f(x)=x^{64}+x^{46}+x^4+x+1$ initial vector is 0xa294d3d7487098b5)

к максимальному значению, что формально соответствует «высокой случайности» по критерию равномерности распределения символов. При этом полученная характеристика оказывается неинформативной, поскольку несмотря на наличие явных закономерностей, присущих натуральному ряду, методика расчета энтропии Шеннона не приводит к заметной деградации частотного распределения состояний. Иными словами, энтропия Шеннона в рассматриваемой постановке слабо чувствительна к наличию упорядоченности и зависимости между элементами, поэтому не выявляет детерминизм последовательности натуральных чисел (рис. 10).

В противоположность этому спектральная энтропия демонстрирует устой-

чиво пониженные значения и существенную вариативность при изменении длины слова, что указывает на концентрацию спектральной энергии в ограниченном числе частотных компонент и, следовательно, на наличие регулярной (квазипериодической) структуры, характерной для неслучайных последовательностей. Наиболее показательным является случай длины слова 20 бит, соответствующей исходному представлению чисел: именно при этом разбиении спектральная энтропия достигает минимума (порядка 0,083), что интерпретируется как максимальная выявляемость детерминированной компоненты временного ряда в естественной для этой разрядности шкале.

Одним из ключевых преимуществ спектральной энтропии является ее низ-

кая зависимость от размера битового слова. Это свойство позволяет добиться более стабильных результатов при анализе данных, независимо от выбранной группировки бит.

На рис. 11 показана взаимосвязь спектральной энтропии и размера битового слова. Ось X отображает размер слова, измеряемый в битах, в пределах от 1 до 65, в то время как ось Y показывает значения

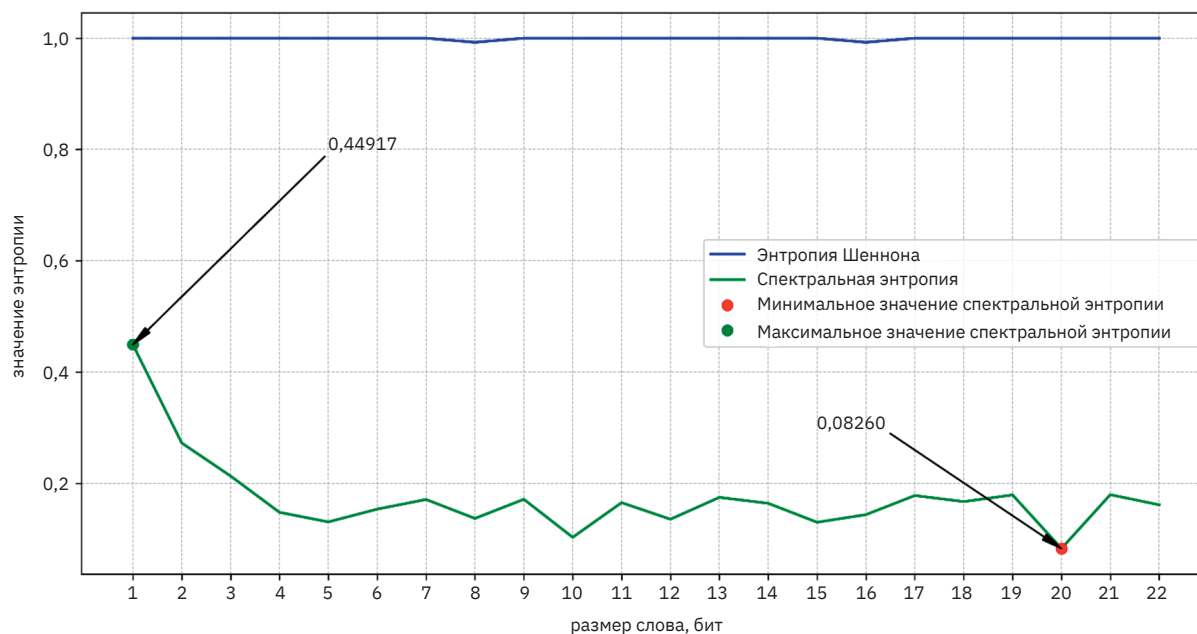


Рис. 10 | Сравнение спектральной энтропии и энтропии Шеннона на различной длине битового слова

Fig. 10 | Comparison of the spectral entropy and Shannon entropy on different length of a word

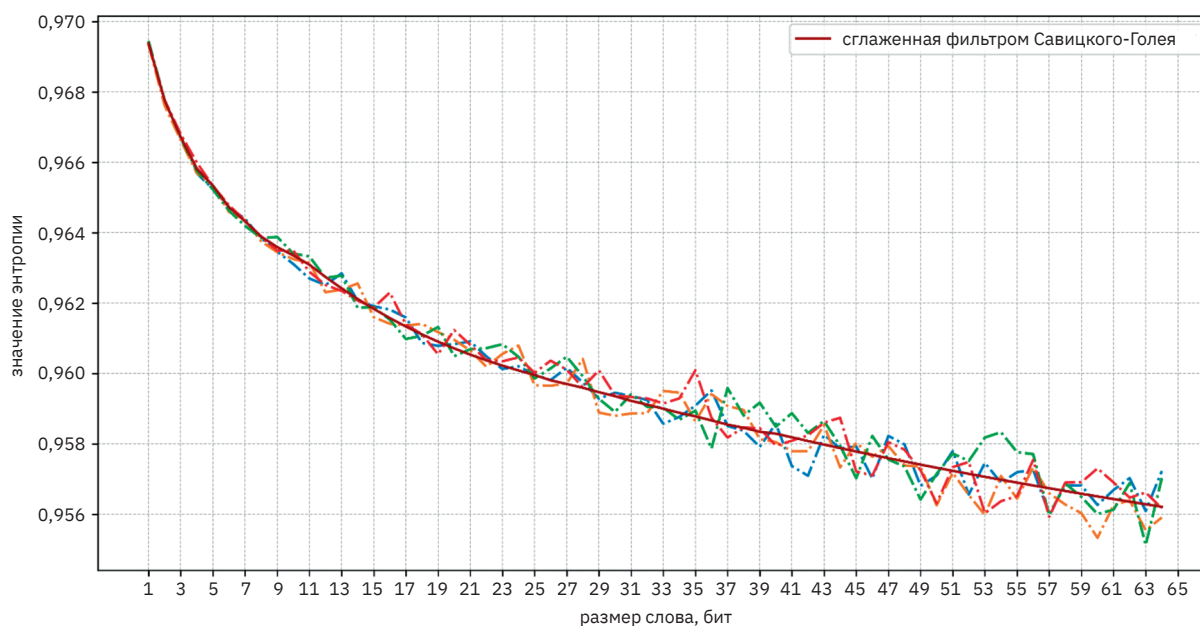


Рис. 11 | Спектральная энтропия в зависимости от размера слова

Fig. 11 | Spectral entropy as a function of word size

энтропии, которые колеблются в диапазоне приблизительно от 0,956 до 0,970.

График демонстрирует, что несмотря на колебания между различными значениями, спектральная энтропия остается в основном стабильной и существенно не меняется с изменением размера слов. Наличие сглаженной линии, полученной с помощью фильтра Савицкого – Голея, подчеркивает этот аспект, производя визуально ровное представление данных. Такое поведение спектральной энтропии свидетельствует об ее устойчивости к вариациям в параметрах, связанных с битовой группировкой. Это делает спектральную энтропию более подходящей для анализа и сравнения структур сложных сигналов и битовых последовательностей, поскольку она позволяет минимизировать влияния, связанные с выбором размерности слова.

Сравнение энтропии Шеннона и спектральной энтропии в зависимости от размера битового слова. Спектральная энтропия представляет собой численное значение, характеризующее уровень неопределенности в распределении вероятностей спектральных компонент сиг-

налов. В отличие от энтропии Шеннона, которая оценивает информацию на основе частоты появления различных битовых слов в выборке, спектральная энтропия демонстрирует более высокую устойчивость к выбору параметров битовой группировки и конечной длине выборки.

Данная устойчивость проявляется в том, что спектральная энтропия сохраняет более стабильные значения, даже при изменении размера слова. Это связано с тем, что она учитывает не только частотное распределение, но и спектральные свойства, что делает ее более чувствительной к структуре в целом. Наоборот, энтропия Шеннона, будучи непосредственно зависимой от частот битовых слов, подвержена значительным колебаниям в зависимости от выбранного размера слова и объема выборки. На рис. 10 показаны значения энтропии Шеннона и спектральной энтропии в зависимости от размера битового слова. Ось X представляет собой размер слова, выражаемый в битах, в диапазоне от 1 до 65. Ось Y показывает соответствующие значения энтропии. График иллюстрирует явную разницу между двумя способами вычисления энтропии, укрепляя аргумент

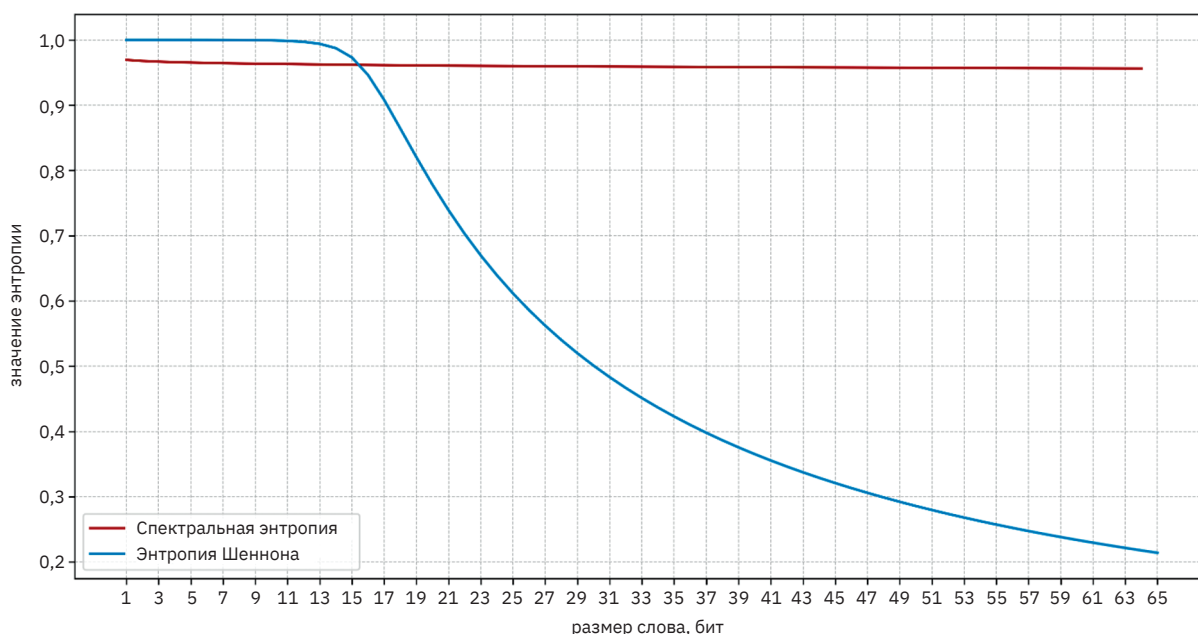


Рис. 12 | Зависимость спектральной энтропии и энтропии Шеннона в зависимости от размера слова

Fig. 12 | Dependence of spectral entropy and Shannon entropy on word size

о том, что спектральная энтропия может служить более надежным инструментом оценки сложности и структуры битовых последовательностей, независимо от размеров слов и длины выборки.

5. ОБСУЖДЕНИЕ

Полученные данные демонстрируют обоснованность перехода от привычного использования исключительно временно-частотного анализа распределений битовых слов к применению частотно-энергетических характеристик. В частности, спектральная энтропия, рассчитанная на основе нормированной спектральной плотности мощности, служит прямым индикатором наличия регулярных компонент и корреляционной структуры в выходном сигнале Г(П)СЧ. В отличие от классической энтропии Шеннона, которая определяется на основе эмпирических частот появления битовых последовательностей и, таким образом, существенно зависит от выбранного размера слова, а также от конечности выборки, спектральная энтропия опирается на агрегированное распределение мощности по отдельным частотным отсчетам. Это приводит к формированию оценки, демонстрирующей более устойчивое поведение при варьировании параметров разбиения и формированию выборок. Приведенная особенность является принципиально важной для решения прикладных задач, где ограниченность доступных данных сочетается с жесткими требованиями по воспроизводимости результатов, что особенно актуально в условиях проведения сертификационных испытаний.

В качестве примера иллюстрации данного подхода приводится детерминированная последовательность натуральных чисел, представляемая в фиксированном двоичном формате. При оценке энтропии Шеннона, основанной на частотном распределении битовых слов и анализе вариантов разбиения, наблюдается формирование заключения, приближающегося к интерпретации «максимальной случай-

ности». Данный эффект объясняется квазирегулярным заполнением блоков, при котором распределение комбинаций может приближаться к равномерному по своим частотным характеристикам. Однако спектральная энтропия стабильно фиксирует несоответствие случайному процессу, поскольку систематичность приращения определяется наличием периодических или квазипериодических компонентов, что приводит к неравномерности спектральной плотности мощности. Снижение энтропии нормированного спектра является следствием этих особенностей. Таким образом, представленный пример подчеркивает методологически значимый эффект, заключающийся в том, что частотные показатели, полученные в пространстве слов, имеют тенденцию «маскировать» детерминированность, в то время как спектральные характеристики позволяют выявить структурные зависимости, которые не обязательно выражаются в виде простого дисбаланса между нулями и единицами или же отклонений частот отдельных блоков.

Особое внимание заслуживает сравнительный анализ предложенного критерия с действующими практиками статистического тестирования, среди которых необходимо выделить методику NIST STS. Эксперимент, проведенный с использованием физического генератора, сертифицированного регулирующим органом, показал, что при неудачном выборе рабочей точки устройство может формально удовлетворять критериям прохождения тестирования по NIST STS, однако при этом продемонстрировать статистически значимое отклонение по параметру спектральной энтропии. После корректировки рабочей точки наблюдалось согласованное улучшение. Как значения спектральной энтропии приходили в рамки допустимого диапазона, так и показатели по стандарту NIST STS демонстрировали улучшение. Преимущество предлагаемого метода состоит в его направленности на контроль именно физически обусловленных деградаций случайности (некорректная рабочая точка), а также в способности выявлять

спектральные аномалии, которые могут не проявляться в виде статистически значимых отклонений в рамках стандартных критериев NIST при конечных объемах данных. Это делает метод спектральной энтропии более пригодным для оперативного мониторинга корректности режима работы физического генератора и для раннего обнаружения перехода источника в нештатное состояние, потенциально приводящее к снижению истинной энтропии при формальном прохождении традиционных тестов случайности.

Построение решающего правила на основе непараметрического бутстреп-оценивания и последующего применения расстояния Махаланобиса обеспечивает формальную статистическую интерпретацию результата тестирования как задачи проверки согласия с эталонной моделью. Бутстреп-процедура позволяет получать эмпирические оценки распределения целевых статистик без введения жестких параметрических предположений о виде закона распределения спектральной энтропии [34], что особенно важно при конечных длинах выборок, наличии корреляций и потенциальной негауссовости. Кроме того, она дает конструктивный механизм построения доверительных областей и порогов при фиксированном протоколе сегментации данных. Использование двумерного признакового пространства (среднее и медиана спектральной энтропии) позволяет одновременно учитывать центральную тенденцию и робастную характеристику распределения значений энтропии по фрагментам, что снижает чувствительность к единичным выбросам и асимметрии распределений.

Применение метрики Махаланобиса обеспечивает корректное агрегирование признаков с учетом их взаимной коррелированности и различной дисперсии [35], т.е. реализует масштабно-инвариантное расстояние в «отбеленном» пространстве признаков и тем самым позволяет сравнивать наблюдаемую точку с эталонным облаком не по покомпонентным порогам, а по единому согласованному критерию, эквивалентному проверке принадлежности доверительному эллипсоиду.

Введение дополнительного контроля однородности по реализациям (квантильная проверка и робастная фильтрация по межквартильному размаху) усиливает практическую применимость методики, поскольку исключает ситуацию, когда приемлемые агрегированные оценки достигаются за счет компенсации локальных деградаций качества «хорошими» участками выборки. К возможным ограничениям подхода относятся: вычислительные затраты бутстреп-процедуры при больших объемах данных и числе регенераций, зависимость получаемых порогов и формы доверительной области от выбранного протокола сегментации и состава эталонных генераторов, а также чувствительность метрики Махаланобиса к качеству оценки ковариационной матрицы (в частности, при малом числе фрагментов или близкой к вырожденной ковариации), что в ряде случаев может требовать робастных или регуляризованных оценок ковариации.

Следует отметить, что результаты, полученные для программных ГПСЧ, требуют корректной интерпретации с учетом методологических предпосылок исследования. Фиксация факта соответствия алгоритма ChaCha20 по критерию спектральной энтропии в рамках принятого протокола свидетельствует об отсутствии статистически детектируемых отклонений от эталонной области, заданной на базе выбранных референсных генераторов и процедуры сегментации данных. Это обстоятельство указывает на то, что спектральная энтропия должна рассматриваться не только как индикатор «слабости» генератора, но и как чувствительный критерий, отражающий особенности реализации устройства, его режим работы, а также условия формирования тестовых данных. Практическое значение данного наблюдения формулируется следующим образом: при выявлении статистически значимого несоответствия по спектральной энтропии генератор необходимо классифицировать как не удовлетворяющий предъявляемым требованиям, что предполагает последующую дисквалификацию устройства для использования

в критически важных криптографических приложениях до проведения дополнительной верификации. Такая проверка должна включать всесторонний анализ параметров и сопоставление с расширенным набором независимых показателей случайности. Результаты сравнительного анализа в работах [36, 37] подтверждают вывод о необходимости осторожной интерпретации данных спектрального анализа в контексте комплексной оценки качества генераторов.

На основании представленного исследования можно сделать вывод о целесообразности применения предложенного подхода в качестве дополнительного слоя контроля качества в задачах криптографической генерации. Внедрение спектральной энтропии в систему тестирования позволяет выявлять спектрально обусловленные аномалии, критичные для безопасности применения криптографических алгоритмов. Разработанный метод, сочетающий в себе анализ распределения мощности в частотной области с применением робастных статистических методов, оказывается способной обнаружить структурные зависимости, не выявляемые стандартными батареями тестов, что позволяет повысить надежность криптографических систем. Результаты демонстрируют, что дополнительная диагностика на базе спектрального анализа способна указывать на необходимость корректировки рабочих точек аппаратных генераторов для достижения оптимальной стабильности и безопасности работы устройств.

В совокупности полученные результаты обоснованно рекомендуют использование спектральной энтропии в качестве дополнительного инструмента контроля качества при оценке как аппаратных, так и программных источников случайности, что имеет большое значение для задач обеспечения криптографической безопасности.

6. ЗАКЛЮЧЕНИЕ

Предложен метод оценки качества генераторов (псевдо-)случайных чисел, ба-

зирующийся на вычислении спектральной энтропии нормализованной спектральной плотности мощности, полученной посредством применения преобразования Фурье, а также на построении статистически обоснованного алгоритма принятия решения, реализованного с применением бутстреп-подхода и метрики Махаланобиса.

Применяемые методы статистической обработки, подтвержденные бутстреп-анализом и вычислением метрики Махаланобиса, создают надежную базу для доказательной характеристики параметров генерации случайных чисел. Экспериментальные данные и сопоставление с аналогичными исследованиями подтверждают объективность предложенного решения, позволяя рекомендовать его для дальнейших исследований в области информационной безопасности. Представленный метод способствует повышению достоверности оценивания за счет снижения зависимости от параметров битового слова и повышения устойчивости к ограниченному объему выборки.

Предложенный метод демонстрирует способность выявлять режимные дефекты физических источников энтропии, которые могут оставаться незамеченными в рамках традиционных наборов статистических тестов. В ходе исследования установлено, что применение энтропии Шеннона, оцениваемой по частотам битовых слов, к детерминированной последовательности натуральных чисел может приводить к ошибочному заключению об «абсолютной случайности» анализируемого ряда. В противоположность этому спектральная энтропия позволяет стабильно обнаруживать принципиальную неслучайность посредством выявления регулярной структуры в частотной области. В рамках проведенного эксперимента ГПСЧ на основе ChaCha20 удовлетворил критерию спектральной энтропии, в связи с чем по результатам настоящей методики он рекомендуется к использованию в криптографических приложениях без дополнительного анализа.

Выявленная зависимость между структурными особенностями спектральной

плотности мощности и качеством генерируемых последовательностей позволяет рекомендовать данный метод для внедрения в процедуру сертификации генераторов в условиях ограниченного объема измерений, где традиционные статистические процедуры могут оказаться недостаточно информативными.

Таким образом, разработанный метод является практически ценным дополнением к существующим инструментам анализа случайных процессов и способствует развитию теории и повышению безопасности криптографических систем за счет повышения качества выявления дефектов в работе генераторов случайных чисел.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. Будько М. Б., Будько М. Ю., Гирик А. В., Грозов В. А. Методы генерации и тестирования случайных последовательностей. СПб: Университет ИТМО, 2019. 70 с. EDN: PAPQUQ.
2. Карпов А. В., Ишмуратов Р. А. Введение в криптографию : Учебное пособие. Казань : Казан. ун-т, 2024. 128 с.
3. Макаренко С. И. Системы спутниковой связи общего пользования и специального назначения: монография. СПб. : Научное издательство «Лань», 2025. 222 с.
4. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М. : КУДИЦ-Образ, 2003. Кн. 2. 240 с.
5. Грищенко А. Ю., Арустамов С. А., Коробейников А. Г., Козин О. В. Защита канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 2. С. 280–291. DOI: 10.17586/2226-1494-2019-19-2-280-291.
6. Грищенко А. Ю. Численное решение многомерной Проблемы Томсона для упаковки векторов на гиперсфере в задачах широкополосной радиосвязи // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 4. С. 730–739. DOI: 10.17586/2226-1494-2019-19-4-730-739. EDN: OIAJHE.
7. Касьянов А. В. Проблема анализа генераторов (псевдо-)случайных чисел // Научно-технический вестник Поволжья. 2024. № 7. С. 292–298. EDN: EFBCOZ.
8. Shannon C. E. A Mathematical Theory of Cryptography (No. 20878). Bell Labs, New Jersey. URL: https://www.academia.edu/41111174/A_Mathematical_Theory_of_Cryptography (дата обращения: 13.03.2026).
9. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal. 1948. Vol. 27. № 3. P. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.
10. Shannon C. E. Communication Theory of Secrecy Systems // The Bell System Technical Journal. 1949. Vol. 28. № 4. P. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.
11. Sönmez M., Elaine T., Kelsey B. J. et al. Recommendation for the Entropy Sources Used for Random Bit Generation. Computer Security. NIST, 2018. 84 p. DOI: 10.6028/NIST.SP.800-90B.
12. Saarinen M.-J. O. SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful. URL: <https://eprint.iacr.org/2022/169.pdf> (дата обращения: 13.03.2026).
13. Goldberg I., Wagner D. Randomness and the Netscape Browser // Dr. Dobbs's Journal. 1996. P. 66–70. URL: <https://people.eecs.berkeley.edu/~daw/papers/ddj-netscape.html> (дата обращения: 13.03.2026).
14. Takeshi N., Hiroyuki S. Analysis of a Security Incident of Open Source Middleware – Case Analysis of 2008 Debian Incident of OpenSSL // 2009 Ninth Annual International Symposium

- on Applications and the Internet, 20–24 July 2009, Bellevue, WA, USA. 2009. P. 247–250. DOI: 10.1109/SAINT.2009.73.
15. **Баранова Е. А., Степанов В. В.** Бэкдоры в криптографических системах: обзор уязвимостей алгоритма DUAL EC DRBG // Теория и практика современной науки. 2017. № 4 (22). С. 991–995.
 16. **Mostafa Hassan.** Cracking Random Number Generators using Machine Learning – Part 1: xorshift128. URL: <https://www.nccgroup.com/research-blog/cracking-random-number-generators-using-machine-learning-part-1-xorshift128/> (дата обращения: 13.03.2026).
 17. **Mostafa Hassan.** Cracking Random Number Generators using Machine Learning – Part 2: Mersenne Twister. URL: <https://www.nccgroup.com/research-blog/cracking-random-number-generators-using-machine-learning-part-2-mersenne-twister/> (дата обращения: 13.03.2026).
 18. CVE-2023-39910 Detail. URL: <https://nvd.nist.gov/vuln/detail/CVE-2023-39910> (дата обращения: 13.03.2026).
 19. **Якубов В. П.** Статистическая радиофизика. Томск : Изд-во НТЛ, 2006. 132 с.
 20. **Гагарин К. Ю.** Математические модели и быстрые алгоритмы векторно-разностного кодирования цифровых речевых сигналов // Информационно-управляющие системы. 2005. № 1 (14). С. 2–9.
 21. **Гимпилович Ю. Б.** Сигналы и процессы в радиоэлектронике. Севастополь : СевГУ, 2019. 247 с.
 22. **Pyt'ev Y. P.** Mathematical Methods of Subjective Modeling in Scientific Research. 2: Applications // Moscow University Physics Bulletin. 2018. Vol. 73. № 2. P. 125–140. DOI: 10.3103/S0027134918020145.
 23. **Pan Y. N., Chen J., Li X. L.** Spectral Entropy: A Complementary Index for Rolling Element Bearing Performance Degradation Assessment // Proceedings of the Institution of Mechanical Engineers. Part C: Journal of Mechanical Engineering Science. 2009. Vol. 223. Iss. 5. P. 1223–1231. DOI: 10.1243/09544062JMES1224.
 24. **Эфрон Б.** Нетрадиционные методы многомерного статистического анализа : пер. с англ. М. : Финансы и статистика, 1988. 263 с.
 25. **Дементьев В. А.** Статистическая процедура бутстреп как средство от многих проблем использования классических законов распределения // Вестник науки и образования. 2023. № 8(139). С. 5–10.
 26. **Касьянов А. В., Витчак И. Д., Еремук В. В.** Минимальная длина битовых последовательностей для асимптотических статистических тестов в криптографии // Правовая информатика. 2025. № 4. С. 79–85. DOI: 10.24412/1994-1404-2025-4-79-85. EDN: TSTHWP.
 27. **Khachumov M. V.** Distances, metrics and cluster analysis // Scientific and Technical Information Processing. 2012. Vol. 39. P. 310–316. DOI: 10.3103/S0147688212060020.
 28. **Etherington T. R.** Mahalanobis distances for ecological niche modelling and outlier detection: implications of sample size, error, and bias for selecting and parameterising a multivariate location and scatter method // PeerJ. 2021. Vol. 9. P. e11436. DOI: 10.7717/peerj.11436.
 29. **Дорофеев В. С., Волосатова Т. М.** Ансамблирование методов обнаружения выбросов при подготовке обучающей выборки данных // Моделирование, оптимизация и информационные технологии. 2022. Т. 10. № 3(38). С. 22–23. DOI: 10.26102/2310-6018/2022.38.3.013.
 30. **Rukhin A., Soto J., Nechvatal J. et al.** A Statistical Test Suite for Random and Pseudorandom Generators for Cryptographic Applications. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (дата обращения: 13.03.2026).
 31. **Bernstein D. J.** ChaCha, a variant of Salsa20. URL: <https://theswissbay.ch/pdf/Crypto/ChaCha%2C%20a%20variant%20of%20Salsa20%20-%20Daniel%20J.%20Bernstein.pdf> (дата обращения: 13.03.2026).
 32. **Bastos D. C., Brasil Kowada L. A., Machado R. C. S.** On pseudorandom number generators // Acta IMEKO. 2020. Vol. 9. № 4. С. 128. DOI: 10.21014/acta_imeko.v9i4.730.
 33. **Cotrina G., Peinado A., Ortiz A.** Gaussian Pseudorandom Number Generator Using Linear Feedback Shift Registers in Extended Fields // Mathematics. 2021. Vol 9. P. 556. DOI: 10.3390/math9050556.
 34. **Hernández W., Calderón-Córdova C., González-Posada V. et al.** Bootstrap-based frequency estimation method // Measurement. 2017. Vol. 95. P. 193–200. DOI: 10.1016/j.measurement.2016.10.012.
 35. **Хаммуд А.** Улучшение процесса принятия многокритериальных решений: новый подход к обобщенным решающим правилам

с использованием расстояния Махалано-биса // *Cifra. Компьютерные науки и информатика*. 2024. № 3 (3). DOI: 10.60797/COMP.2024.3.2. EDN: XVACNU.

36. **Чижма С. Н., Газизов Р. И.** Анализ точности метода спектрального анализа сигналов в системах электроснабжения // Омский на-

учный вестник. 2013. № 1 (117). С. 202–206. EDN: QJIPUL.

37. **Силин Н. В.** Электромагнитный контроль электротехнического оборудования // Вестник Дальневосточного государственного технического университета. 2010. № 2(4). С. 35–42. EDN: OYJHBJ.

REFERENCES

1. **Budko M. B., Budko M. Yu., Girik A. V., Grozov V. A.** Methods for Generating and Testing Random Sequences. St. Petersburg : Universitet ITMO, 2019, 70 p. EDN: PAPQUQ. (In Russian)
2. **Karpov A. V., Ishmuratov R. A.** Introduction to Cryptography : A Study Guide. Kazan : Kazanskij universitet, 2024, 128 p. (In Russian)
3. **Makarenko S. I.** Satellite communication systems for general and specific purposes. St. Petersburg, Naukoemkie Tehnologii Publ., 2025, 222 p. (In Russian)
4. **Ivanov M. A., Chugunkov I. V.** Theory, Application, and Quality Assessment of Pseudorandom Sequence Generators. Moscow : KUDIC-Obraz, 2003. Book 2, 240 p. (In Russian)
5. **Grishentsev A. Yu., Arustamov S. A., Korobeynikov A. G., Kozin O. V.** Orthogonal noise-like signal symbols for broadband channel protection. *Scientific and technical journal of information technologies, mechanics and optics*. 2019. Vol. 19. No. 2, pp. 280–291. DOI: 10.17586/2226-1494-2019-19-2-280-291. (In Russian)
6. **Grishentsev A. Yu.** Numerical solution of multidimensional thomson problem for vectors packaging on hypersphere in broadband radiocommunication problems. *Technical journal of information technologies, mechanics and optics*. 2019. Vol. 19. No. 4, pp. 730–739. DOI: 10.17586/2226-1494-2019-19-4-730-739. EDN: OIAJHE. (In Russian)
7. **Kasyanov A. V.** The problem of analysing generators of (pseudo-) random numbers. *Scientific and technical Volga region bulletin*. 2024. No. 7, pp. 292–298. EDN: EFBCOZ. (In Russian)
8. **Shannon C. E.** A Mathematical Theory of Cryptography (No. 20878). Bell Labs, New Jersey. URL: https://www.academia.edu/41111174/A_Mathematical_Theory_of_Cryptography (accessed: 13.03.2026).
9. **Shannon C. E.** A Mathematical Theory of Communication. *The Bell System Technical Journal*. 1948. Vol. 27. No. 3, pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.
10. **Shannon C. E.** Communication Theory of Secrecy Systems. *The Bell System Technical Journal*. 1949. Vol. 28. No. 4, pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.
11. **Sönmez M., Elaine T., Kelsey B. J. et al.** Recommendation for the Entropy Sources Used for Random Bit Generation. Computer Security. NIST, 2018, 84 p. DOI: 10.6028/NIST.SP.800-90B.
12. **Saarinen M.-J. O.** SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful. URL: <https://eprint.iacr.org/2022/169.pdf> (accessed: 13.03.2026).
13. **Goldberg I., Wagner D.** Randomness and the Netscape Browser. *Dr. Dobbs's Journal*. 1996, pp. 66–70. URL: <https://people.eecs.berkeley.edu/~daw/papers/ddj-netscape.html> (accessed: 13.03.2026).
14. **Takeshi N., Hiroyuki S.** Analysis of a Security Incident of Open Source Middleware – Case Analysis of 2008 Debian Incident of OpenSSL. 2009 Ninth Annual International Symposium on Applications and the Internet, 20–24 July 2009, Bellevue, WA, USA. 2009, pp. 247–250. DOI: 10.1109/SAINT.2009.73.
15. **Baranova E. A., Stepanov V. V.** Backdoors in cryptographic systems: a review of the vulnerabilities of the DUAL EC DRBG algorithm. *Teoriya i praktika sovremennoj nauki*. 2017. No. 4 (22), pp. 991–995. (In Russian)
16. **Mostafa Hassan.** Cracking Random Number Generators using Machine Learning – Part 1: xorshift128. URL: <https://www.nccgroup.com/research-blog/cracking-random-number-generators-using-machine-learning-part-1-xorshift128/> (accessed: 13.03.2026).

17. **Mostafa Hassan.** Cracking Random Number Generators using Machine Learning – Part 2: Mersenne Twister. URL: <https://www.nccgroup.com/research-blog/cracking-random-number-generators-using-machine-learning-part-2-mersenne-twister/> (accessed: 13.03.2026).
18. CVE-2023-39910 Detail. URL: <https://nvd.nist.gov/vuln/detail/CVE-2023-39910> (accessed: 13.03.2026).
19. **Yakubov V. P.** Statistical radiophysics. Tomsk : Izd-vo NTL, 2006, 132 p. (In Russian)
20. **Gagarin K. Yu.** Mathematical models and fast algorithms of vector-differential coding of digital speech signals. *Information and control systems*. 2005. No. 1 (14), pp. 2–9. (In Russian)
21. **Gimpilevich Yu. B.** Signals and processes in radio electronics. Sevastopol: SevGU, 2019, 247 p. (In Russian)
22. **Pyt'ev Y. P.** Mathematical Methods of Subjective Modeling in Scientific Research. 2: Applications. *Moscow University Physics Bulletin*. 2018. Vol. 73. No. 2, pp. 125–140. DOI: 10.3103/S0027134918020145.
23. **Pan Y. N., Chen J., Li X. L.** Spectral Entropy: A Complementary Index for Rolling Element Bearing Performance Degradation Assessment. *Proceedings of the Institution of Mechanical Engineers. Part C: Journal of Mechanical Engineering Science*. 2009. Vol. 223. Iss. 5, pp. 1223–1231. DOI: 10.1243/09544062JMES1224.
24. **Efron B.** Nonparametric estimates of standard error: the jackknife, the bootstrap and other methods. CA: Stanford Univ., 1980, 647 p.
25. **Dementiev V. A.** Statistical bootstrap procedure as a remedy for many problems of using classical distribution laws. *Vestnik nauki i obrazovaniya*. 2023. No. 8(139), pp. 5–10. (In Russian)
26. **Kasyanov A. V., Vitchak I. D., Eremuk V. V.** Minimum length of bit sequences for asymptotic statistical tests in cryptography. *Legal Informatics*. 2025. No. 4, pp. 79–85. DOI:10.24412/1994-1404-2025-4-79-85.EDN: TSTHWP. (In Russian)
27. **Khachumov M. V.** Distances, metrics and cluster analysis. *Scientific and Technical Information Processing*. 2012. Vol. 39, pp. 310–316. DOI: 10.3103/S0147688212060020.
28. **Etherington T. R.** Mahalanobis distances for ecological niche modelling and outlier detection: implications of sample size, error, and bias for selecting and parameterising a multivariate location and scatter method. *PeerJ*. 2021. Vol. 9, pp. e11436. DOI: 10.7717/peerj.11436.
29. **Dorofeev V. S., Volosatova T. M.** Ensemble methods for detecting outliers in the preparation of a training data set. *Modeling, Optimization and Information Technology*. 2022. Vol. 10. No. 3(38), pp. 22–23. DOI: 10.26102/2310-6018/2022.38.3.013. (In Russian)
30. **Rukhin A., Soto J., Nechvatal J. et al.** A Statistical Test Suite for Random and Pseudorandom Generators for Cryptographic Applications. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762 (accessed: 13.03.2026).
31. **Bernstein D. J.** ChaCha, a variant of Salsa20. URL: <https://theswissbay.ch/pdf/Crypto/ChaCha%2C%20a%20variant%20of%20Salsa20%20-%20Daniel%20J.%20Bernstein.pdf> (accessed: 13.03.2026).
32. **Bastos D. C., Brasil Kowada L. A., Machado R. C. S.** On pseudorandom number generators. *Acta IMEKO*. 2020. Vol. 9. No. 4, pp. 128. DOI: 10.21014/acta_imeko.v9i4.730.
33. **Cotrina G., Peinado A., Ortiz. A.** Gaussian Pseudorandom Number Generator Using Linear Feedback Shift Registers in Extended Fields. *Mathematics*. 2021. Vol 9. P. 556. DOI: 10.3390/math9050556.
34. **Hernández W., Calderón-Córdova C., González-Posada V. et al.** Bootstrap-based frequency estimation method. *Measurement*. 2017. Vol. 95, pp. 193–200. DOI: 10.1016/j.measurement.2016.10.012.
35. **Hammoud A.** Enhancing multi-criteria decision-making: a novel approach to generalized decision rules using Mahalanobis distance. *Cifra. Computer sciences and informatics*. 2024. No. 3 (3). DOI: 10.60797/COMP.2024.3.2. EDN: XVACNU. (In Russian)
36. **Chizhma S. N., Gazizov R. I.** Analysis of the accuracy of the method of spectral analysis of signals in power systems. *Omsk scientific bulletin*. 2013. No. 1 (117). pp. 202–206. EDN: QJIPUL. (In Russian)
37. **Silin N. V.** Electromagnetic control of electrotechnical equipment. *Vestnik Dal'nevostochnogo gosudarstvennogo tekhnicheskogo universiteta*. 2010. No. 2(4), pp. 35–42. EDN: OYJHBJ. (In Russian)

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

КАСЬЯНОВ Александр Владимирович – аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Россия, 197022, Санкт-Петербург, ул. Профессора Попова, д. 5, лит. Ф; научный сотрудник, ООО «Специальный Технологический Центр» (ООО «СТЦ»), Санкт-Петербург, 195220, пр-т Непокоренных, д. 17, к. 4, лит. В, пом. 3Н
E-mail: kasjanov@inbox.ru
ORCID: 0009-0000-3319-8357

ГРИШЕНЦЕВ Алексей Юрьевич – д-р техн. наук, чл.-кор. академии электротехнических наук РФ, доцент, Национальный исследовательский университет ИТМО, Россия, 197101, Санкт-Петербург, Кронверкский пр-т, д. 49, лит. А
E-mail: agrishentsev@yandex.ru
ORCID: 0000-0003-1373-0670

KASYANOV Alexandr V. – Postgraduate Student, Saint Petersburg Electrotechnical University, Russia, 197022, St. Petersburg, Professora Popova str., 5, bldg. F; Researcher, Special Technology Center LLC (STC LLC), St. Petersburg, 195220, Nepokoronykh ave., 17/4, bldg. B

GRISHENTSEV Alexey Yu. – Doctor of Engineering Sciences, Corresponding member of the Russian Academy of Electrotechnical Sciences, Associate Professor, ITMO University, Russia, 197101, St. Petersburg, Kronverksky ave., 49, bldg. A