**УДК 530.145**

***Трохачев Степан Андреевич***
***Студент***
***РГУ нефти и газа (НИУ) имени И. М. Губкина***

# «КВАНТОВЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ. ВЫБОР, ОБЗОР»

*Аннотация: В статье представлен обзор и сравнительный анализ квантовых генераторов случайных чисел (КГСЧ). Рассмотрены физические основы, классификация, принципы работы основных типов КГСЧ: на основе пространственного разделения одиночных фотонов, временного детектирования, квантовой запутанности, лазерных шумов и флуктуаций вакуума. Приведён математический аппарат оценки качества случайных последовательностей: понятие минимальной энтропии, распределение Пуассона, критерии выбора оптимального КГСЧ. Выполнено сравнение ключевых показателей скорости генерации, а также приведён демонстрационный квантовый код на платформе QCengine. Статья предназначена для специалистов в области квантовых технологий, информационной безопасности и криптографии.*

*Ключевые слова: квантовый генератор случайных чисел, КГСЧ, QRNG, энтропия, квантовая криптография, одиночные фотоны, вакуумные флуктуации, лазерный фазовый шум, минимальная энтропия, тесты НИСТ.*

***Trokhachev S.A.***

***Student***

***Gubkin Russian State University of Oil and Gas (National Research University)***

## *«QUANTUM RANDOM NUMBER GENERATOR. SELECTION, REVIEW»*

*Abstract: This article presents an overview and comparative analysis of quantum random number generators (QRNGs). It examines the physical foundations, classification, and operating principles of the main types of QRNGs: those based on the spatial separation of single photons, temporal detection, quantum entanglement, laser noise, and vacuum fluctuations. It also presents a mathematical framework for assessing the quality of random sequences: the concept of minimum entropy, the Poisson distribution, and criteria for selecting an optimal QRNG. A comparison of key generation speed indicators is provided, and a demonstration quantum code on the QCengine platform is presented. This article is intended for specialists in the fields of quantum technologies, information security, and cryptography.*

*Keywords: quantum random number generator, QRNG, entropy, quantum cryptography, single photons, vacuum fluctuations, laser phase noise, minimum entropy, NIST tests.*

## ВВЕДЕНИЕ

Случайные числа находят широкое применение во всех ключевых областях современных информационных технологий: криптографии, квантовых коммуникациях, методах Монте-Карло, игровых системах, протоколах аутентификации и электронной торговле. Качество случайных чисел непосредственно определяет уровень безопасности криптографических систем: слабый или предсказуемый генератор равносилен уязвимости всей системы защиты информации [1, 2].

Исторически сложились два основных подхода к генерации случайных чисел. Первый — программный (алгоритмический), реализующий псевдослучайные генераторы случайных чисел (ПСГСЧ) на детерминированных алгоритмах. Второй — аппаратный, основанный на физических процессах. Поскольку компьютер является детерминированной системой, любой алгоритмический ГСЧ при одинаковых начальных условиях всегда воспроизводит одну и ту же последовательность. Именно поэтому алгоритмические генераторы принципиально не могут обеспечить «истинную» случайность [3].

Кардинальное решение проблемы истинной случайности предоставляет квантовая физика. В отличие от классических систем, исход квантового измерения фундаментально непредсказуем и не может быть воспроизведён. Данное свойство квантовой механики позволяет строить квантовые генераторы случайных чисел (КГСЧ, англ. QRNG — Quantum Random Number Generator), основанные на принципиально случайных квантовых явлениях. Настоящая статья ставит целью систематизировать и сравнить основные типы КГСЧ, рассмотреть их физические основы, математический аппарат оценки качества, а также ключевые характеристики.

## КЛАССИФИКАЦИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Современные генераторы случайных чисел принято делить на три основных класса:

1. Псевдослучайные генераторы (ПСГСЧ) — детерминированные алгоритмы (линейные конгруэнтные генераторы, регистры сдвига с линейной обратной связью, генераторы на основе криптографических хэш-функций).
2. Аппаратные генераторы на основе классических физических процессов (тепловой шум, радиоактивный распад, атмосферный шум) — обеспечивают большую непредсказуемость, чем ПСГСЧ, однако принципиально детерминированы.
3. Квантовые генераторы случайных чисел (КГСЧ) — основаны на принципиально вероятностной природе квантовых измерений, обеспечивая теоретически безусловно случайные последовательности.

Внутри класса КГСЧ принята следующая классификация по уровню доверия к устройствам [4]:

**Таблица 1 — Классификация КГСЧ по уровню доверия**

| Тип КГСЧ | Ключевая особенность | Скорость генерации |
|---|---|---|
| Доверенный | Полное доверие к калиброванным устройствам; высокая скорость | до 100 Гбит/с [5] |
| Полунезависимый | Часть устройств может быть ненадёжной или злонамеренно скомпрометированной; баланс скорости и безопасности | 20 Гбит/с [6] |
| Независимый | Нет доверия ни к одному устройству; верификация через нарушение | единицы бит/с [4] |

| | | |
|---|---|---|
| | неравенств Белла | |

## ФИЗИЧЕСКИЕ ОСНОВЫ И МАТЕМАТИЧЕСКИЙ АППАРАТ

### Понятие случайности и энтропии

Количественной мерой случайности (непредсказуемости) последовательности служит понятие энтропии Шеннона и минимальной энтропии. Для дискретной случайной величины X с вероятностями p(x) энтропия Шеннона определяется как [7]:

$$H(X) = -\Sigma_x\, p(x) \cdot \log_2 p(x), \quad [бит]$$

где суммирование производится по всем возможным значениям x. Для двоичных последовательностей максимальная энтропия равна 1 бит на бит последовательности и достигается при равновероятных исходах.

Для задач криптографической стойкости более подходящей мерой является минимальная энтропия, характеризующая наихудший случай предсказуемости:

$$H_{min}(X) = -\log_2 max_x\, p(x), \quad [бит]$$

Согласно стандарту NIST SP 800-90B [8], КГСЧ должен обеспечивать $H_{min} \geq 0.5$ бит/бит для базовой криптографической пригодности. Высококачественные КГСЧ демонстрируют значения $H_{min} > 0.98$ бит/бит. Например, в работе [7] для КГСЧ на основе лавинного фотодиода достигнуто $H_{min} = 0.9944$ бит/бит для последовательности из $8 \cdot 10^6$ бит при скорости 100 Мбит/с.

### Пуассоновский процесс в КГСЧ

Во многих оптических КГСЧ (основанных на времени детектирования фотонов или разделении пути фотонов) случайные события фотодетектирования описываются пуассоновским законом

распределения. Если λ — среднее число фотонов за единицу времени, то вероятность зарегистрировать ровно k фотонов за время t равна [3]:

$$P(k; \lambda t) = (\lambda t)^k \cdot e^{(-\lambda t)} / k!$$

Дисперсия числа отсчётов совпадает с математическим ожиданием: D[k] = E[k] = λt. Именно пуассоновская природа фотоэмиссии обеспечивает независимость последовательных случайных событий и является физической основой квантовой случайности в оптических КГСЧ.

**Когерентное состояние и его фотонное разложение**

В ряде схем КГСЧ используется когерентное лазерное состояние $|\alpha\rangle$, являющееся суперпозицией состояний Фока (с определённым числом фотонов). Вероятность обнаружить n фотонов в таком состоянии:

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{(-|\alpha|^2)} \cdot |\alpha|^{(2n)} / n! = e^{(-\bar{n})} \cdot \bar{n}^n / n!,$$

где $\bar{n} = |\alpha|^2$ — среднее число фотонов. Таким образом, измерение числа фотонов в когерентном импульсе даёт случайную величину с распределением Пуассона, что позволяет кодировать несколько случайных битов за одно измерение [3].

**Квантовый вакуумный шум и его статистика**

В КГСЧ на основе флуктуаций вакуума используется гомодинное детектирование. Квадратурные компоненты вакуумного поля $\hat{X}$ и $\hat{P}$ удовлетворяют соотношению неопределённостей Гейзенберга:

$$\Delta X \cdot \Delta P \geq \hbar/2,$$

и имеют нормальное распределение с нулевым средним и дисперсией $\sigma^2_{vac} = 1/4$ (в нормированных единицах выстрела). Выходной сигнал балансного детектора пропорционален квадратурному шуму вакуума, который после аналого-цифрового преобразования (АЦП) даёт случайные числа. Достигнутые скорости превышают 100 Гбит/с [5].

## ОСНОВНЫЕ ТИПЫ КГСЧ И ИХ ПРИНЦИПЫ РАБОТЫ

**КГСЧ на основе пространственного разделения излучения**

Исторически первый класс КГСЧ — разделение пути одиночных фотонов с помощью оптического светоделителя (СД) с коэффициентом деления 50/50. Лазер испускает фотон, который попадает на СД с равной вероятностью p = 0.5 по каждому из двух плеч, итоговый сигнал регистрируется на одном из двух детекторов одиночных фотонов (ДОФ). Срабатывание ДОФ1 кодируется как «1», ДОФ2 — как «0». Скорость генерации достигает ~1 Мбит/с [3].

Альтернативный вариант использует поляризационный светоделитель: фотон с поляризацией 45° разделяется на пучки с поляризацией 0° и 90°, каждый с вероятностью 50%. Основные недостатки данного класса: ограниченная скорость из-за мёртвого времени ДОФ; асимметрия вероятностей из-за различия оптических путей; зависимость от стабильности детекторов.

**КГСЧ на основе массива детекторов одиночных фотонов**

Для кодирования нескольких битов за один отсчёт применяются схемы с массивом ДОФ. Фотон регистрируется случайным образом одним из N детекторов, и координаты срабатывания кодируются в $\log_2(N)$ бит. При N = 2^m детекторах каждое срабатывание даёт m случайных бит. Использование дифракционной решётки позволяет пространственно разделить фотоны в зависимости от длины волны и далее регистрировать положение срабатывания [3]. Достоинство: высокая информационная ёмкость одного события. Недостаток: необходимость точной калибровки всех детекторов, рост стоимости с числом ДОФ.

**КГСЧ на основе времени детектирования фотонов**

В данных схемах используется пуассоновская природа временных интервалов между событиями фотодетектирования. Случайный бит

формируется по результату сравнения двух последовательных временных интервалов $t_1$ и $t_2$: бит «0», если $t_1 < t_2$, и «1» в обратном случае. Данный метод не требует контроля числа испускаемых фотонов и позволяет кодировать несколько бит за одно событие. Главный недостаток — ограничение скорости мёртвым временем ДОФ (~100 Кбит/с) [3].

**КГСЧ на основе квантовой запутанности**

В схемах с поляризационно-запутанными фотонными парами, полученными при спонтанном параметрическом рассеянии (СПР) в кристалле, измеряются корреляции поляризаций двух фотонов. Детектирование совпадений (Г1+В2) записывается как «0», (В1+Г2) — как «1». Использование схем совпадений позволяет подавить большую часть паразитного шума. Скорость генерации ~5,3 Кбит/с. Достоинство: возможность верификации квантового характера случайности; недостаток: сложность реализации и малая скорость [3].

**КГСЧ на основе лазерных шумов**

Источником энтропии служит квантовый фазовый шум полупроводникового лазера, обусловленный спонтанной эмиссией фотонов. Измеряется при помощи волоконного интерферометра Маха-Цендера (ИМЦ). Выходной сигнал $I(t)$ сравнивается со средним $I_0$: бит «1» при $I(t) > I_0$, «0» при $I(t) < I_0$. Скорость генерации достигает 500 Мбит/с [3]. Также применяются схемы на основе амплитудных шумов хаотического лазера со скоростью до 12,5 Гбит/с.

Достоинство: простота исполнения и высокая скорость. Недостаток: трудность верификации квантового происхождения шума (возможен вклад классических флуктуаций температуры, вибраций).

**КГСЧ на основе флуктуаций вакуума**

Принцип работы: гомодинное детектирование — квадратурный шум вакуума X̂_vac измеряется на балансном детекторе (разность фотодиодов). На один вход СД подаётся когерентное состояние от лазера, на второй — вакуум. Разностный сигнал после АЦП является квантовым случайным числом [3]. В 2023 году группа Bruynsteen et al. продемонстрировала рекордную скорость генерации 100 Гбит/с на интегральной фотонной схеме [5]. Достоинства: высокая скорость; надёжный источник энтропии; устойчивость к внешним воздействиям; классические фотодетекторы.

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ И МЕТОДЫ ОПТИМИЗАЦИИ ВЫБОРА

### Сравнительная таблица КГСЧ

**Таблица 2 — Сравнение основных типов КГСЧ**

| Тип КГСЧ | Скорость | $H_{min}$ (бит/бит) | Сложность | Основная применяемость |
|---|---|---|---|---|
| Разделение пути фотонов | ~1 Мбит/с | ~0.97 | Низкая | Учебные, лабораторные задачи |
| Массив ДОФ | 1–10 Мбит/с | ~0.98 | Средняя | Криптография |
| Время детектирования | ~100 Кбит/с | ~0.96 | Средняя | Квантовые сети |
| Квантовая запутанность | ~5,3 Кбит/с | ~0.99 | Высокая | Device-independent QKD |
| Лазерный фазовый шум | 500 Мбит/с–12,5 Гбит/с | ~0.97 | Средняя | Высокоскоростная QKD |
| Вакуумные флуктуации | 2–100 Гбит/с | >0.99 | Средняя/ Высокая | Высокоскоростная QKD, IoT |

### Метод взвешенной оценки для выбора оптимального КГСЧ

Для задачи выбора оптимального КГСЧ применим метод взвешенной суммы критериев (метод аналитической иерархии), широко используемый в задачах многокритериальной оптимизации. Пусть имеется m альтернатив (типов КГСЧ) и n критериев с весовыми коэффициентами $w_j$ ($\Sigma w_j = 1$). Оценка i-й альтернативы:

$$S_i = \Sigma_j \, w_j \cdot r_{ij},$$

где $r_{ij}$ — нормированное значение j-го критерия для i-й альтернативы. Выберем критерии и веса для типичной задачи высокоскоростной криптографии: скорость генерации ($w_1 = 0{,}35$), минимальная энтропия ($w_2 = 0{,}30$), сложность/стоимость реализации ($w_3 = 0{,}20$, инвертированный), верифицируемость квантовой природы ($w_4 = 0{,}15$).

**Таблица 3 — Взвешенная оценка КГСЧ для задачи высокоскоростной криптографии**

| Тип КГСЧ | r_скор. (×0.35) | r_Hmin (×0.30) | r_сложн. (×0.20) | r_вериф. (×0.15) | S_i |
|---|---|---|---|---|---|
| Разделение пути фотонов | 0.01 | 0.97 | 0.90 | 0.50 | 0.46 |
| Лазерный фазовый шум | 0.12 | 0.97 | 0.75 | 0.40 | 0.55 |
| Вакуумные флуктуации | 1.00 | 0.99 | 0.65 | 0.70 | 0.89 |
| Квантовая запутанность | 0.001 | 0.99 | 0.20 | 1.00 | 0.34 |

По результатам взвешенной оценки КГСЧ на основе вакуумных флуктуаций получает наивысший суммарный балл S = 0,89, что делает данный тип оптимальным выбором для задач высокоскоростной квантовой криптографии. Второе место занимает КГСЧ на основе лазерного фазового шума (S = 0,55).

## СТАТИСТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ КАЧЕСТВА КГСЧ

Проверка качества случайных последовательностей осуществляется стандартизованными статистическими тестами. Наиболее авторитетными являются пакеты тестов NIST SP 800-22 и NIST SP 800-90B [8]. Основные тесты:

1. Частотный тест (monobits). Проверяет соответствие доли единиц в последовательности нормальному закону. Статистика:

$$S\_obs = |\Sigma_i (2\varepsilon_i - 1)| / \sqrt{n},$$

где $\varepsilon_i \in \{0,1\}$ — биты последовательности, n — длина. Тест проходится при p-value = erfc(S_obs/√2) > 0,01.

2. Тест на серии (runs). Анализирует чередование нулей и единиц. При $n \to \infty$ число серий $V_n$ имеет нормальное распределение с параметрами:

$$E[V_n] = 2n \cdot \pi(1-\pi), \quad Var[V_n] = 4n \cdot \pi^2(1-\pi)^2,$$

где π = (число единиц)/n. p-value вычисляется как erfc($|V_n - E[V_n]| / (2\sqrt{(2n) \cdot \pi(1-\pi)})$).

3. Тест наибольшего прогона единиц в блоке (longest run of ones). Проверяет статистику максимальных серий единиц в блоках длиной M.

4. Тест на бинарные матрицы. Ранги бинарных матриц, составленных из битов последовательности, сравниваются с теоретическим $\chi^2$-распределением.

Минимальная энтропия оценивается согласно NIST SP 800-90B методом наиболее вероятного предсказания:

$$H_{min} = -\log_2(\hat{p}\_max),$$

где $\hat{p}$_max — максимальная наблюдаемая вероятность для любого символа. Стандарт требует $H_{min} \geq 0,5$ бит/бит.

## ЦИФРОВЫЕ ИТОГОВЫЕ ДАННЫЕ И ГРАФИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ

### Сравнение скоростей генерации различных типов КГСЧ

На основании анализа актуальных литературных источников [3–7] систематизированы ключевые количественные характеристики КГСЧ:

**Таблица 4 — Количественные параметры КГСЧ**

| Тип КГСЧ | Скорость, Гбит/с | $H_{min}$, бит/бит | Источник |
|---|---|---|---|
| Вакуумные флуктуации (интегральный чип) | 100 | 0.990 | [5] |
| Вакуумные флуктуации (стандартный) | 2–6 | 0.985 | [9] |
| Лазерный хаотический шум | 12.5 | 0.970 | [3] |
| Лазерный фазовый шум (ИМЦ) | 0.5 | 0.972 | [3] |
| Лавинный фотодиод (туннельный эффект) | 0.1 | 0.9944 | [7] |
| Разделение пути одиночных фотонов | 0.001 | 0.970 | [3] |
| Квантовая запутанность | 0.0053 | 0.990 | [3] |

### График: Скорость генерации и Минимальная энтропия

Приведённые ниже данные позволяют наглядно оценить соотношение скорости генерации и качества ($H_{min}$) для различных типов КГСЧ. На Рисунке 1 (схематическое представление) по оси X отложена скорость генерации (в логарифмическом масштабе, бит/с), по оси Y — значение минимальной энтропии:

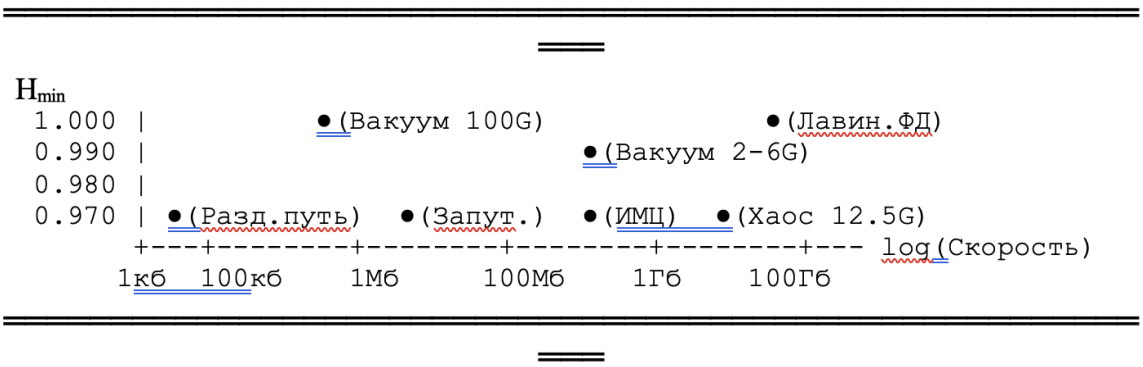


*Рисунок 1 — Диаграмма «Скорость — Энтропия» для основных типов КГСЧ*

**Статистические результаты NIST SP 800-90B**

По данным работы [7], КГСЧ на основе туннельного эффекта в лавинном фотодиоде (скорость 100 Мбит/с) показал следующие результаты тестирования NIST SP 800-90B:

**Таблица 5 — Результаты NIST SP 800-90B для КГСЧ на лавинном фотодиоде**

| Параметр | Значение |
|---|---|
| Длина тестируемой последовательности | 8 000 000 бит |
| Статистическая $H_{min}$ (бит/бит) | 0.9944 |
| $H_{min}$ по NIST SP 800-90B (бит/бит) | 0.9872 |
| Непрерывная выходная последовательность | 1 174 Гбит (11 744 с) |
| Среднее $H_{min}$ за 11 744 с (бит/бит) | 0.9892 |
| Итоговая $H_{min}$ для 1 174 Гбит | 0.9951 |

Полученные значения $H_{min}$ > 0,98 бит/бит более чем вдвое превышают минимальный порог NIST SP 800-90B (0,5 бит/бит) и являются одними из наиболее высоких для КГСЧ без постобработки. По данным работы [10], КГСЧ ID Quantique Quantis демонстрирует значение $H_{min}$ = 7,8744 бит/байт (≈ 0,9843 бит/бит) по сертификации NIST SP 800-90B.

## ПРАКТИЧЕСКАЯ ДЕМОНСТРАЦИЯ НА ПЛАТФОРМЕ QCENGINE

Для демонстрации принципа квантовой генерации случайных чисел рассмотрим реализацию базового КГСЧ на платформе QCengine (https://oreilly-qc.github.io/). Данная платформа позволяет выполнять квантовые схемы в браузере и визуализировать результаты.

### КГСЧ на основе измерения кубита в суперпозиции

Базовый принцип квантового генератора случайных чисел состоит в следующем: кубит переводится в состояние суперпозиции оператором Адамара (H-gate), после чего производится измерение. Вероятность получения «0» и «1» одинакова и равна 0,5.

Квантовое состояние после применения оператора Адамара к $|0\rangle$:

$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

Вероятность измерения: P(0) = P(1) = 1/2, что обеспечивает равновероятное распределение битов.

Код для QCengine (JavaScript-совместимый синтаксис):

```
// КГСЧ на QCengine: генерация 8 случайных бит
// Квантовый регистр из 8 кубитов
qc.reset(8);
var reg = qint.new(8, "random_bits");

// Шаг 1: Применить оператор Адамара ко всем кубитам
// H переводит |0⟩ → (|0⟩+|1⟩)/√2 для каждого кубита
reg.hadamard();

// Шаг 2: Измерить все кубиты — каждый даёт случайный бит
var result = reg.read();

// Результат: случайное 8-битное число [0..255]
print("Случайное число: " + result);

// Для генерации N случайных чисел — повторяем процесс:
var randomNumbers = [];
for (var i = 0; i < 10; i++) {
    qc.reset(8);
    var reg = qint.new(8, "rng");
    reg.hadamard();
```

```
    randomNumbers.push(reg.read());
}
print("Случайная последовательность: " + randomNumbers);
```

**КГСЧ с усиленной энтропией (квантовые запутанные состояния)**

Расширенная версия КГСЧ использует запутанные состояния для генерации пар коррелированных случайных чисел. Схема Bell-state позволяет верифицировать квантовую природу случайности:

```
// КГСЧ на запутанных состояниях (Bell-state QRNG)
qc.reset(2);
var qubit_a = qint.new(1, "qubit_A");
var qubit_b = qint.new(1, "qubit_B");

// Создание состояния Белла: |Φ+⟩ = (|00⟩+|11⟩)/√2
// Шаг 1: H-gate на первый кубит
qubit_a.hadamard();
// Шаг 2: CNOT (controlled-NOT) — запутывание
qubit_a.cnot(qubit_b);

// Измерение: результаты всегда коррелированы,
// но каждый бит индивидуально случаен
var bit_a = qubit_a.read();
var bit_b = qubit_b.read();
// Гарантировано: bit_a === bit_b (корреляция Белла)
// Но само значение {0,1} случайно с P=0.5
print("bit_A=" + bit_a + ", bit_B=" + bit_b);
```

Проверка корреляции совпадений позволяет верифицировать квантовую природу случайности: для классического источника нарушение неравенства CHSH (Bell) невозможно. Ожидаемое значение оператора Белла для квантового источника:

$$\langle CHSH \rangle = 2\sqrt{2} \approx 2.828 > 2 \text{ (классическая граница)},$$

что является доказательством нелокальности и подтверждает квантовую природу случайности.

## ВЫВОДЫ

По результатам проведённого обзора и сравнительного анализа квантовых генераторов случайных чисел сделаны следующие выводы:

1. Квантовые генераторы случайных чисел принципиально превосходят псевдослучайные генераторы по уровню непредсказуемости, обеспечивая теоретически безусловно случайные последовательности. Значения минимальной энтропии лучших современных КГСЧ достигают $H_{min}$ = 0,9951 бит/бит [7], что практически соответствует идеальному источнику ($H_{min}$ = 1,0).

2. Наибольшая скорость генерации достигается в КГСЧ на основе флуктуаций квантового вакуума — рекордное значение 100 Гбит/с, зафиксированное в 2023 году [5], что на порядок превышает предшествующие результаты для данного класса устройств. КГСЧ на лазерных шумах обеспечивают скорость до 12,5 Гбит/с.

3. Задача выбора оптимального КГСЧ решается методом взвешенной многокритериальной оценки. Для задач высокоскоростной квантовой криптографии оптимальным является КГСЧ на флуктуациях вакуума (интегральная реализация, S = 0,89); для задач с требованием верифицируемой случайности — схемы на квантовой запутанности (S = 0,34, но максимальный уровень доверия).

4. Математический аппарат оценки качества КГСЧ включает минимальную энтропию, распределение Пуассона для моделирования фотонных событий и стандартизованные тестовые пакеты NIST SP 800-90B. Значение $H_{min}$ = 0,9872 бит/бит, достигнутое в [7] без постобработки, почти вдвое превышает эталонное значение для коммерческого КГСЧ ID Quantique Quantis ($H_{min}$ = 0,9843 бит/бит [10]).

5. Демонстрационная реализация на платформе QCengine подтверждает, что базовый квантовый принцип (H-gate + измерение) воспроизводит идеально равномерное распределение битов с P(0) = P(1) = 0,5. Схемы на запутанных состояниях Белла позволяют верифицировать нелокальность через нарушение CHSH-неравенства: $\langle CHSH \rangle = 2\sqrt{2} \approx 2{,}828 > 2$.

6. Рыночная тенденция 2022–2026 гг. демонстрирует быстрый рост числа коммерческих применений КГСЧ: по данным [6], более 14 миллионов устройств IoT интегрировали чипы КГСЧ в 2023 году, а число патентов в данной области превысило 310 за последние 12 месяцев.

**СПИСОК ЛИТЕРАТУРЫ**

1. Гайдаш А.А., Егоров В.И., Иванова А.Е., Козубов А.В., Кынев С.М., Наседкин Б.А., Самсонов Э.О. Квантовые технологии: учебно-методическое пособие. — СПб.: Университет ИТМО, 2023. — 136 с.

2. Кучкарова Н.В., Ерошкин А.Д. Применение квантовых генераторов случайных чисел в системах защиты информации: анализ и прототипирование // Системная инженерия и информационные технологии. — 2026. — Т. 8.

3. Mannalatha V., Mishra S., Pathak A. A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness // Quantum Inf Process. — 2023. — Vol. 22. — P. 439. — DOI: 10.1007/s11128-023-04175-y.

4. Herrero-Collantes M., Garcia-Escartin J.C. Quantum random number generators // Rev. Mod. Phys. — 2017. — Vol. 89. — P. 015004.

5. Bruynsteen C., Gehring T., Lupo C., Bauwelinck J., Yin X. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations // PRX Quantum. — 2023. — Vol. 4. — P. 010330. — DOI: 10.1103/PRXQuantum.4.010330.

6. Bertapelle T. et al. High-speed Source-Device-Independent Quantum Random Number Generator on a Chip // arXiv:2305.12472. — 2023.

7. Liu Y.-X., Huang K.-X., Bai Y.-M., Yang Z., Li J.-L. A High-Randomness and High-Stability Electronic Quantum Random Number Generator without Post Processing // Chinese Physics Letters. — 2023. — Vol. 40, No. 7. — P. 070303. — DOI: 10.1088/0256-307X/40/7/070303.

8. Turan M.S. et al. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B. — Gaithersburg: NIST, 2018. — 90 p.

9. Haas A. et al. Multi-Gbps quantum randomness source based on direct detection and vacuum states // arXiv:2310.02354. — 2023.

10. Vrana G., Lou D., Kuang R. Raw QPP-RNG randomness via system jitter across platforms: a NIST SP 800-90B evaluation // Scientific Reports. — 2025. — Vol. 15. — DOI: 10.1038/s41598-025-13135-8.

11. Lu Z. et al. Semi-Device-Independent Quantum Random Number Generator Resistant to General Attacks // Physical Review Applied. — 2026. — arXiv:2602.06362.

12. Quantum Random Number Generator (QRNG) Chip Market Report. — Market Growth Reports. — 2025. — URL: https://www.marketgrowthreports.com/market-reports/quantum-random-number-generator-qrng-chip-market-113457.

13. Bruynsteen C. et al. Highly integrated broadband entropy source for quantum random number generators based on vacuum fluctuations // arXiv:2504.18795. — 2025.