УДК 004.415, 004.056

Т. О. ГОРЕЛІКОВА
Запорізький національний університет
О. В. ЧОПОРОВА
Київський національний економічний університет імені Вадима Гетьмана

ВИСОКОЕНТРОПІЙНІ ВИПАДКОВІ ЧИСЛА ЯК ОСНОВА КРИПТОГРАФІЧНОЇ БЕЗПЕКИ: КВАНТОВИЙ ПІДХІД

У статті представлено систематичне дослідження розробки генератора випадкових чисел з високою ентропією, що базується на фізичних процесах квантової природи. Потреба в надійній випадковості обґрунтована з точки зору сучасних криптографічних застосувань, у яких якість згенерованих послідовностей відіграє вирішальну роль у забезпеченні інформаційної безпеки. Зокрема, увага приділяється обмеженням існуючих підходів, включаючи псевдовипадкові алгоритми.

Як альтернативу пропонується підхід, який використовує флуктуації електричних сигналів, спричинені дискретною природою носіїв заряду у фотодетекторі. Ці флуктуації інтерпретуються як фундаментальне джерело ентропії, оскільки вони виникають внаслідок ймовірнісних процесів, які неможливо змоделювати детерміновано. У дослідженні описано теоретичні основи цього явища та проаналізовано можливості практичної реалізації в рамках інтегрованої системи. Запропонована система складається з кількох функціональних компонентів, включаючи сенсорну підсистему для виявлення фізичного шуму, аналоговий ланцюг обробки для посилення та фільтрації, а також цифровий модуль для перетворення сигналу та подальшої обробки. Особлива увага приділяється використанню кількох незалежних каналів, що сприяє стійкості та стабільності згенерованого виходу. Крім того, застосовуються методи пост-обробки для корекції статистичних відхилень та забезпечення рівномірного розподілу згенерованих значень.

Експериментальні результати демонструють, що згенеровані послідовності відповідають вимогам високої ентропії, однорідності та незалежності. Статистичний аналіз підтверджує, що вихід не має значних кореляцій або структурних відхилень, що підкреслює придатність системи для криптографічних застосувань. Також продемонстровано, що запропоноване рішення практично здійсненне з використанням поширених електронних компонентів та може бути гнучко інтегровано в існуючі цифрові інфраструктури.

Поєднання фундаментальної фізики та технічної реалізації дозволяє досягти високого рівня безпеки та непередбачуваності, що є важливим з огляду на зростаючі вимоги до інформаційної безпеки та постійний технологічний прогрес.

Ключові слова: *квантовий генератор випадкових чисел, висока ентропія, фотонний шум, дробовий шум, криптографічна безпека, генерація випадкових чисел, фізичне джерело ентропії, обробка сигналів, постобробка, статистичний аналіз, інформаційна безпека, апаратна реалізація, системи на основі мікроконтролерів, цифрова криптографія.*

T. O. HORELIKOVA
Zaporizhzhia National University
O. V. CHOPOROVA
Kyiv National Economic University named after Vadym Hetman

HIGH-ENTROPIC RANDOM NUMBERS AS THE BASIS OF CRYPTOGRAPHIC SECURITY: A QUANTUM APPROACH

The article presents a systematic study of the development of a high-entropy random number generator based on physical processes of quantum nature. The need for reliable randomness is justified from the point of view of modern cryptographic applications, in which the quality of the generated sequences plays a crucial role in ensuring information security. In particular, attention is paid to the limitations of existing approaches, including pseudo-random algorithms. As an alternative, an approach is proposed that uses fluctuations in electrical signals caused by the discrete nature of charge carriers in the photodetector. These fluctuations are interpreted as a fundamental source of entropy, since they arise from probabilistic processes that cannot be modeled deterministically. The study describes the theoretical foundations of this phenomenon and analyzes the possibilities of practical implementation within the framework of an integrated system. The proposed system consists of several functional components, including a sensor subsystem for detecting physical noise, an analog processing circuit for amplification and filtering, and a digital module for signal conversion and further processing. Special attention is paid to the use of multiple independent channels, which contributes to the robustness

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

and stability of the generated output. In addition, post-processing methods are used to correct statistical deviations and ensure a uniform distribution of the generated values.

Experimental results demonstrate that the generated sequences meet the requirements of high entropy, homogeneity, and independence. Statistical analysis confirms that the output does not have significant correlations or structural deviations, which emphasizes the suitability of the system for cryptographic applications. It is also demonstrated that the proposed solution is practically feasible using common electronic components and can be flexibly integrated into existing digital infrastructures.

The combination of fundamental physics and technical implementation allows achieving a high level of security and unpredictability, which is important in view of the growing requirements for information security and constant technological progress.

Keywords: *quantum random number generator, high entropy, photon noise, fractional noise, cryptographic security, random number generation, physical source of entropy, signal processing, post-processing, statistical analysis, information security, hardware implementation, microcontroller-based systems, digital cryptography.*

Постановка проблеми

У сучасній цифровій екосистемі інформаційна безпека є фундаментальною основою стабільної роботи як цивільних, так і промислових систем. Експоненціальне зростання потоків даних, широке впровадження розподілених мереж та розвиток інфраструктури на основі блокчейну призвели до значного зростання вимог щодо криптографічної надійності. Автор статті у своєму методі захисту даних у контексті блокчейну віддає якості випадкових чисел центральне місце, оскільки вони формують основу для ключового матеріалу, протоколів автентифікації та цифрових підписів [1–2].

Проблема надійної випадковості має не лише технічний характер, а й торкається основи сучасної криптографії. Багато існуючих систем використовують генератори псевдовипадкових чисел, які застосовують детерміновані алгоритми для створення послідовностей, що виглядають статистично випадковими. Незважаючи на їхню ефективність, такі підходи залишаються принципово обмеженими, оскільки їхній вихід відтворюваний, коли відомий внутрішній стан або початкові параметри. Це означає, що безпека цих систем залежить від припущень щодо обчислювальної складності, які залежать від технологічного прогресу.

Вразливість псевдовипадкових значень була продемонстрована історично в різних реальних ситуаціях, де криптографічні системи були скомпрометовані передбачуваними ключами або недостатньою ентропією.

Наприклад:

– проблема з RSA-ключами в мікросхемах Infineon (2017);

– помилка в Debian OpenSSL (2008);

– уразливість Bitcoin-гаманців на Android (2013);

– недолік ідентифікаторів сесій у PHP (2007).

Такі інциденти підкреслюють, що навіть невеликі відхилення від ідеальної випадковості можуть призвести до непропорційно великих ризиків для безпеки. У критичних застосуваннях, таких як фінансові транзакції, управління ідентифікацією та розподілені механізми консенсусу, це може призвести до втрати конфіденційності, цілісності та доступності [3].

На цьому тлі виникає потреба в розробці альтернативних підходів, які не залежать від детермінованих моделей чи класичної системи. Перспективним напрямком є використання процесів на квантовому рівні, де невизначеність є внутрішньою властивістю і не виникає з неповних знань. Це означає, що випадковість не моделюється чи апроксимується, а виникає безпосередньо з фундаментальної структури природи.

Тим не менш, практична реалізація таких підходів створює нові виклики. Забезпечення стабільності, відтворюваності статистичних властивостей та інтеграції в існуючі цифрові системи вимагає ретельного поєднання фізичних, електронних та обчислювальних компонентів.

Отже, суть проблеми полягає в розробці надійного джерела високої ентропії, яке, з одного боку, базується на принципово непередбачуваних процесах, а з іншого, придатне

для практичного застосування в сучасних інформаційних системах. Вирішення цієї проблеми є важливим для посилення стійкості цифрових інфраструктур до поточних і майбутніх загроз.

Аналіз сучасних досліджень та публікацій

У сучасній цифровій інфраструктурі надійність криптографічних механізмів є фундаментальною передумовою захисту даних. Якість випадкових чисел відіграє вирішальну роль у цьому контексті, оскільки вони безпосередньо впливають на безпеку криптографічних ключів, протоколів автентифікації та цифрових підписів. У науковій літературі неодноразово наголошується, що недостатня ентропія у згенерованих послідовностях може призвести до структурних вразливостей у системах безпеки.

Традиційно розрізняють генератори псевдовипадкових чисел та фізично обґрунтовані методи. Генератори псевдовипадкових чисел базуються на детермінованих алгоритмах, які створюють, здавалося б, випадкові послідовності, починаючи з початкового стану. Незважаючи на їхню високу ефективність та широке застосування, численні дослідження демонструють, що такі системи залишаються за своєю суттю передбачуваними, коли стають відомими внутрішні параметри або початкові значення. Дослідження показали, що цей тип генератора призвів до серйозних інцидентів безпеки в багатьох випадках, коли криптографічні ключі могли бути реконструйовані [4].

У відповідь на це були розроблені криптографічно захищені генератори, які використовують складні математичні структури та важкорозв'язні задачі. Хоча цей підхід значно підвищує практичну безпеку, він залишається залежним від припущень щодо обчислювальної складності. Однак, постійний розвиток обчислювальної потужності та алгоритмічних інновацій, включаючи зростання швидкості обчислень, викликає питання щодо довгострокової стійкості цього підходу [5].

Паралельно науковцями досліджуються апаратні генератори випадкових чисел, що використовують фізичні процеси, такі як тепловий шум, електричні коливання або електромагнітні хаотичні зміни. Ці системи зазвичай пропонують вищий ступінь ентропії, ніж алгоритмічні рішення. Тим не менш, нещодавні публікації вказують на кілька обмежень, включаючи чутливість до зовнішніх впливів, нестабільність умов вимірювання та наявність прихованих кореляцій у згенерованих сигналах [6]. Як наслідок, формально гарантувати абсолютну випадковість залишається складним.

На відміну від класичних систем, де невизначеність часто виникає через складність або неповні знання, випадковість у квантових процесах є невід'ємною властивістю природи. Різні дослідження описують реалізації, засновані, серед іншого, на поляризації фотонів, спонтанному випромінюванні та квантовому тунелюванні. Ці підходи дозволяють генерувати випадковість, яка є принципово непередбачуваною, навіть за умови повного знання системи [7].

У цій галузі досліджень особливу увагу приділяють використанню так званого дробового шуму у фотодетекторах. Цей вид шуму виникає через дискретну природу носіїв заряду та характеризується статистичною незалежністю від окремих подій. Публікації демонструють, що такі сигнали, за умови їх правильного посилення та обробки, можуть служити надійним джерелом високої ентропії. Водночас наголошується, що для усунення будь-якої асиметрії в необроблених даних необхідні додаткові методи корекції зміщення [8].

Підсумовуючи, можна стверджувати, що кожен з існуючих підходів має свої переваги та обмеження. Сучасна тенденція в наукових дослідженнях зосереджена на гібридних системах. Зокрема, квантові методи пропонують перспективний напрямок для розробки надійних та перспективних генераторів випадкових чисел, придатних для застосувань з високими вимогами безпеки.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Мета дослідження

Основною метою цього дослідження є розробка та обґрунтування надійної концепції генерації випадкових чисел з високим ступенем ентропії, що базується на фундаментальних фізичних процесах. Зокрема, це дослідження зосереджено на використанні квантово-механічних явищ як внутрішнього джерела непередбачуваності з кінцевою метою підвищення безпеки та стійкості сучасних криптографічних систем, зокрема системи блокчейн.

У контексті інформаційної безпеки якість випадковості є критичним параметром. Зрештою, згенеровані значення безпосередньо використовуються в таких процесах, як генерація ключів, автентифікація та цифровий підпис. Тому метою цього дослідження є не лише реалізація функціональної системи, але й демонстрація того, що отримана випадковість відповідає статистичним та теоретичним критеріям, необхідним для застосувань у системах, що вимагають високий рівень безпеки.

Важливим аспектом мети є аналіз обмежень існуючих методів генерації випадкових чисел. Як алгоритмічні, так і класичні апаратні підходи розглядаються з точки зору передбачуваності, чутливості до зовнішніх впливів та структурних недоліків. На основі цього аналізу метою є формулювання альтернативи, яка мінімізує ці обмеження, використовуючи фізичну основу, в якій випадковість не моделюється, а є невід'ємною частиною [9].

Особлива увага приділяється процесам, що виникають через дискретну природу елементарних частинок, оскільки ці процеси характеризуються фундаментальною невизначеністю. Вибір такого джерела вимагає ретельної оцінки стабільності, відтворюваності та стійкості до зовнішніх факторів.

Задача полягає в розробці інтегрованої системної архітектури, в якій фізичне джерело випадковості поєднується з електронними та обчислювальними компонентами. Це передбачає розробку ланцюга обробки сигналів, здатного підсилювати слабкі та шумоподібні сигнали, оцифровувати їх та перетворювати на придатні для використання двійкові послідовності. Важливо, щоб обробка не вводила нових кореляцій і щоб початкова ентропія максимально зберігалася.

Окрім апаратної реалізації, автор також зосередився на розробці методів статистичної корекції та оптимізації згенерованих даних. Оскільки фізичні процеси на практиці часто демонструють невеликі відхилення або зміщення, необхідно застосовувати методи, які усувають ці нерівності, не порушуючи самої випадковості. Результатом дослідження є отримання вихідної послідовності, яка задовольняє критерії рівномірного розподілу та властивості незалежності.

Ще однією важливою частиною роботи є оцінка якості згенерованої випадковості. Це включає застосування методів статистичного тестування та аналіз таких параметрів, як ентропія, рівномірність розподілу та відсутність кореляцій. За допомогою цієї оцінки можна визначити, наскільки запропонована система придатна для практичного застосування в криптографії та інформаційній безпеці.

Крім того, невід'ємною задачею є забезпечення практичного застосування розробленої системи. Це означає, що рішення має бути не лише теоретично обґрунтованим, але й здійсненним з використанням стандартних електронних компонентів та інтегрованим в існуючі цифрові інфраструктури. Масштабованість, енергоефективність та економічна ефективність є важливими передумовами в цьому відношенні.

Підсумовуючи, метою цього дослідження є розробка інноваційного та науково обґрунтованого рішення для генерації випадкових чисел з високими значеннями. Використовуючи квантові явища та інтегрований системний підхід, метою є значний внесок у подальший розвиток безпечних та надійних криптографічних технологій.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Виклад основного матеріалу дослідження

Основний принцип запропонованого методу базується на виявленні флуктуацій (невеликих випадкових коливань або змін у часі або просторі), що виникають через дискретну природу електричного заряду. Коли фотодетектор піддається впливу низької інтенсивності світла або навіть працює в умовах мінімального зовнішнього випромінювання, генеруються електричні сигнали, що виникають внаслідок дії окремих носіїв заряду. Ці носії заряду не рухаються безперервно, а виглядають як окремі події, що підлягають розподілу ймовірностей. Це створює струм, який змінюється випадково та не має передбачуваної закономірності.

Фізичне походження цих флуктуацій полягає в тому, що взаємодія між фотонами та напівпровідниковим матеріалом не є детермінованою (такою, що підпорядковується певним законам і передбачувана).

Коли фотон досягає фотодетектора, процес розпізнавання окремих фотонів визначається не класичною фізикою, а квантовою статистикою. Це призводить до так званих флуктуацій дробового шуму, які складають фундаментальну ентропію системи. При взаємодії світлового сигналу з фотоприймачем кількість зареєстрованих подій підпорядковується закону Пуассона. Використовуючи цей розподіл, можна обчислити ймовірність того, що пристрій вловить саме k фотонів за конкретне часове вікно за формулою:

$$P(k;\lambda)=\frac{\lambda^k e^{-\lambda}}{k!}, \tag{1}$$

де λ – середня інтенсивність фотонного потоку.

Кожну подію виявлення можна вважати незалежною реалізацією ймовірнісного процесу. Це означає, що навіть за повного знання макроскопічних параметрів системи, таких як температура, напруга та інтенсивність світла, точний час та інтенсивність окремої події неможливо передбачити. Ця властивість є основою для генерації справжньої випадковості.

Статистичний опис процесу виявлення можна апроксимувати за допомогою моделей, у яких визначено ймовірність спостереження певної кількості подій протягом часового інтервалу. Результуючий потік містить шумову складову, спектральна щільність якої пов'язана із середньою швидкістю потоку. Ця шумова складова вважається основним джерелом ентропії в системі. Для перевірки ступеня хаотичності згенерованих даних застосовують ентропійний аналіз за Шенноном. Розрахунок проводиться за такою залежністю:

$$H(x)=-\sum_{i=1}^{n} p_i \log_2 p_i, \tag{2}$$

де p_i відображає ймовірність виникнення конкретного символу в наборі. У разі ідеальної роботи генератора показник ентропії сягає свого максимуму, що фактично означає наявність одного повного біта інформації в кожному згенерованому біті послідовності.

Щоб зробити цю ентропію практично придатною для використання, необхідно відповідним чином обробляти аналоговий сигнал. Необроблений сигнал, що походить від фотодетектора, зазвичай має дуже низький рівень і не може бути використаний безпосередньо для цифрових застосувань. Тому вводиться фаза посилення, в якій сигнал посилюється без порушення основних статистичних властивостей. Це вимагає використання малошумних підсилювачів, щоб власні коливання системи залишалися домінуючими над зовнішніми впливами.

Посилені сигнали згодом фільтруються для придушення небажаних частотних складових. Ця фільтрація є важливою для мінімізації перешкод, що виникають з навколишнього середовища, таких як електромагнітні перешкоди або тепловий дрейф. Вибір характеристик фільтра має бути ретельно узгоджений з властивостями шумового процесу, щоб зберегти відповідну інформацію [10].

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Після аналогової обробки сигнал оцифровується за допомогою аналого-цифрового перетворювача. Це перетворення є вирішальним кроком, оскільки воно визначає, як безперервні коливання перетворюються на дискретні значення. Роздільна здатність та частота дискретизації перетворювача безпосередньо впливають на якість згенерованої двійкової послідовності. Недостатня роздільна здатність може призвести до втрати інформації, тоді як занадто низька частота дискретизації може призвести до кореляції між послідовними вимірюваннями.

У цифровій області отриманий сигнал додатково обробляється для отримання двійкового представлення. Це передбачає використання порогових значень або диференціальних методів для перетворення аналогових варіацій у дискретні біти. Дуже важливо, щоб це перетворення не вносило систематичного зміщення, оскільки це зменшило б ентропію вихідного сигналу.

На практиці зміщення фактично неминуче, тому що необроблені дані демонструватимуть невеликі відхилення від ідеального рівномірного розподілу. Ці відхилення можуть виникати через асиметрію обладнання, варіації характеристик компонентів або зовнішні впливи. Для виправлення цих ефектів застосовується етап постобробки, спрямований на усунення статистичного зміщення. Цей етап гарантує, що кінцева двійкова послідовність відповідає вимогам незалежності та рівного розподілу ймовірностей.

Щоб усунути цю проблему, у пристрої використовується алгоритм фон Неймана. Його принцип полягає в наступному: вхідна бітова послідовність ділиться на пари бітів. Після цього пари «00» та «11» ігноруються, а комбінації «01» та «10» перетворюються на нові біти – «01» стає нулем, а «10» – одиницею. Завдяки цьому залишаються тільки біти, що з'являються з однаковою ймовірністю, і усувається будь-який перекіс у джерелі даних. Формально процедура описується таким чином:

$$f\left(b_1,b_2\right)=\begin{cases}\varnothing,\ b_1=b_2\\ 0,\left(b_1,b_2\right)=\left(0,1\right)\\ 1,\ \ \left(b_1,b_2\right)=\left(1,0\right)\end{cases}. \tag{3}$$

Отже, навіть якщо початковий фотонний шум має певні закономірності або відхилення, після обробки алгоритмом фон Неймана вихідна послідовність стає рівномірно випадковою [11].

У підсумку, в основі роботи системи лежить використання квантової природи світла та дискретності електричного заряду. Генерація випадковості відбувається шляхом реєстрації дробового шуму – спонтанних флуктуацій струму, що виникають у фотодетекторі під впливом слабкого світлового потоку. Оскільки поява кожного окремого фотона є фундаментально випадковою подією, результуючий сигнал неможливо передбачити детерміновано, що робить його ідеальним джерелом фізичної ентропії.

Процес перетворення цих хаотичних квантових подій у надійний цифровий продукт відбувається за алгоритмом що продемонстрований у таблиці 1.

Практична реалізація запропонованої системи генерації випадкових чисел вимагає інтегрованого підходу, в якому фізичні, електронні та обчислювальні компоненти тісно пов'язані.

Основу системи утворює сенсорна підсистема, відповідальна за виявлення коливань електричних сигналів. Аналоговий каскад реалізовано на операційному підсилювачі малошумного типу (наприклад MOPA2340UA). Як первинний детектор використовується напівпровідниковий компонент, чутливий до слабких світлових сигналів і здатний реєструвати мінімальні коливання струму. Робота цього детектора базується на тому, що навіть за відсутності зовнішнього освітлення залишається невеликий струм, що виникає внаслідок теплових та квантово-механічних ефектів. Цей струм має флуктуючий характер і є початковим джерелом ентропії.

Для забезпечення незалежності від зовнішніх впливів детектор розміщується в екранованому середовищі(захищеному від потрапляння світла із зовні). Це запобігає впливу коливань навколишнього освітлення або електромагнітних перешкод на результати вимірювання. Для

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Таблиця 1

Алгоритм роботи системи генерації випадкових чисел

Крок	Етап процесу	Опис дії	Результат
1	Генерація ентропії	Фотодетектор фіксує слабке світло. Через дискретність фотонів виникають випадкові стрибки струму (дробовий шум)	Сирий фізичний мікросигнал
2	Детекція (Сенсор)	Реєстрація окремих подій, що слідують імовірнісному розподілу (недетермінована природа)	Слабкі аналогові флуктуації
3	Підсилення	Малошумний підсилювач (LNA) збільшує амплітуду сигналу, пригнічуючи зовнішні перешкоди та наводки	Посилений аналоговий шум
4	Дискретизація (АЦП)	Аналого-цифровий перетворювач перетворює неперервний сигнал у послідовність цифрових значень	Потік сирих двійкових даних
5	Паралельний збір	Об’єднання даних з кількох незалежних каналів для підвищення стійкості та обсягу ентропії	Мультиплексований бітовий потік
6	Оцінка якості	Вимірювання ентропії отриманої послідовності та перевірка на наявність закономірностей	Показник ступеня випадковості
7	Постобробка	Вибіркова фільтрація для усунення статистичного зміщення	Очищена рівномірна послідовність
8	Вихід системи	Формування фінальної послідовності бітів, придатної для криптографічного використання	True Random Number

надійності додається контрольоване джерело світла певного спектру, яке забезпечує стабільну базову інтенсивність. Це забезпечує стабільний рівень сигналу, зберігаючи при цьому основні коливання.

Аналоговий сигнал, що генерується детектором, має дуже низький рівень і не може бути використаний безпосередньо для цифрової обробки. Тому використовується схема підсилення, спеціально розроблена для низьких рівнів шуму. Ця схема складається з конфігурації операційного підсилювача, в якій коефіцієнт підсилення був ретельно підібраний, щоб зробити невеликі коливання видимими та запобігти насиченню сигналу. Резистор зворотного зв’язку номіналом 100 кОм визначає величину підсилення, тоді як паралельно ввімкнений конденсатор 100 нФ виконує функцію обмеження високочастотної складової. Повна електрична схема тестового зразка представлена на рисунку 1.

Після аналогової обробки сигнал передається на модуль цифрової обробки. У запропонованому прототипі для цієї мети використовується мікроконтролер, оснащений вбудованим аналого-цифровим перетворювачем. Цей компонент виконує вибірку сигналу та перетворює аналогові значення напруги в цифрові представлення.

Вибір параметрів дискретизації має вирішальне значення для якості згенерованих даних. Занадто низька частота дискретизації може призвести до втрати інформації та потенційних кореляцій між послідовними значеннями. З іншого боку, занадто висока частота може призвести до надмірності та збільшення навантаження на обчислювальну потужність. У розробленій системі було знайдено баланс, який гарантує як ефективність, так і точність.

Після оцифрування сигнал піддається серії операцій, спрямованих на вилучення двійкових значень. Важливою особливістю розробленого прототипу є застосування кількох незалежних каналів детектування. Кожен канал складається з окремого детектора та пов’язаної з ним схеми підсилення. Завдяки паралельному використанню цих каналів підвищується надійність системи та зменшується ймовірність систематичних помилок. Якщо один канал тимчасово демонструє аномальну поведінку, інші канали можуть це компенсувати.

Сигнали з різних каналів об’єднуються за допомогою методів цифрової обробки. Застосовуються методи, що забезпечують придушення локальних відхилень та максимізацію комбінованої ентропії. Цього можна досягти, серед інших методів, за допомогою логічних операцій та процедур статистичного відбору. Фотографію реального прототипу наведено на рисунку 2.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

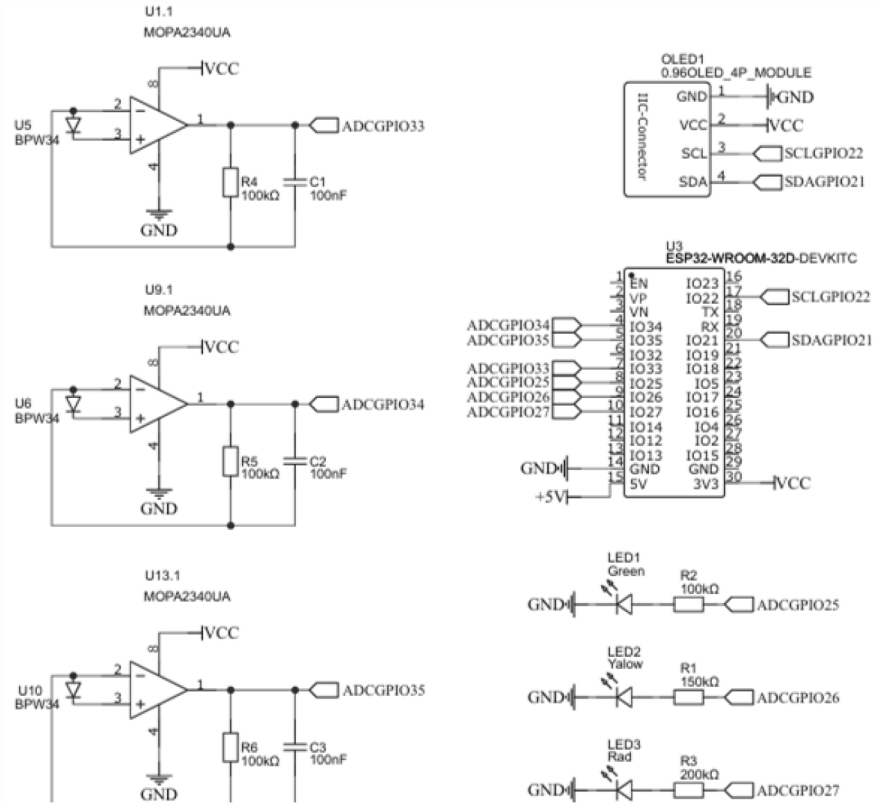

Рис. 1. Електрична схема розробленої системи

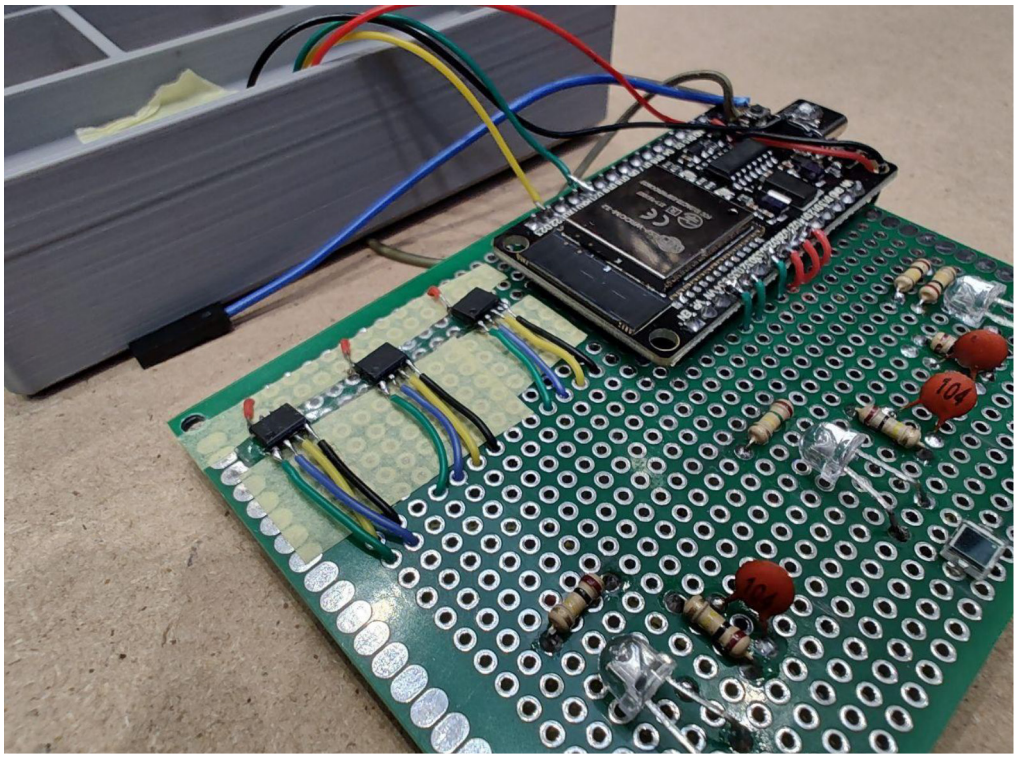

Рис. 2. Прототип апаратного забезпечення з кількома каналами виявлення

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Фізичну реалізацію прототипу системи було здійснено на експериментальній платформі, в яку інтегровані всі компоненти. Прототип включає детектори, схеми підсилення, мікроконтролер та додаткові модулі для зв'язку та візуалізації. Конструкція виконана таким чином, щоб сигнальні шляхи були якомога коротшими для мінімізації шуму та перешкод.

Додатковою частиною тестової системи є модуль відображення, який використовується для демонстраційних цілей. Цей модуль дозволяє відображати згенеровані випадкові значення в режимі реального часу. Хоча це не є важливим компонентом для роботи системи, він пропонує переваги під час тестування та представлення результатів. Фотографія готового демонстраційного варіанта представлена на рисунку 3.

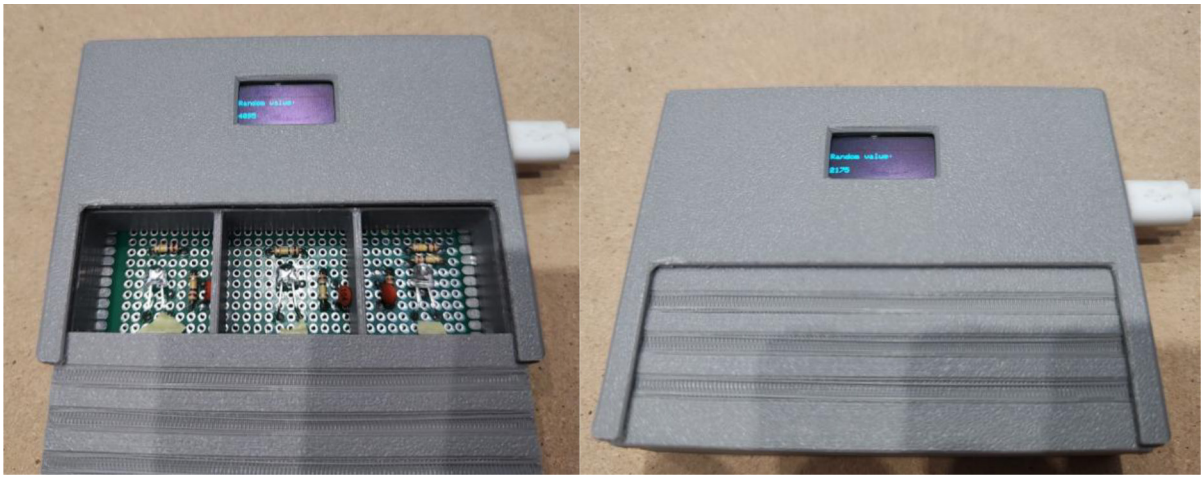

Рис. 3. Реалізація прототипу

На практиці система може взаємодіяти із зовнішніми пристроями через стандартні інтерфейси. Згенеровані дані можна, наприклад, надсилати на комп'ютер або мережевий модуль, де вони використовуються в криптографічних процесах. Це робить систему придатною для інтеграції в ширші архітектури безпеки.

Для оцінки продуктивності системи було проведено серію експериментів, в яких було зібрано великі обсяги даних. Отримані набори даних були проаналізовані за допомогою статистичних методів, спрямованих на виявлення відхилень від ідеальної випадковості. Це включало дослідження розподілу значень, наявності кореляцій та ступеня ентропії. Результати досліджень відображені у таблиці 2.

Таблиця 2

Відповідність експериментальних результатів теоретичним вимогам

Критерій	Теоретична вимога	Отриманий результат	Оцінка
Рівномірність розподілу	Однакова ймовірність значень	Підтверджено χ^2-тестом	Відповідає
Відсутність кореляції	Незалежність значень	Автокореляція ≈ 0	Відповідає
Висока ентропія	Близькість до максимуму	H ≈ 7.97 біт/символ	Відповідає
Відсутність повторів	Мінімізація дублікатів	Повтори відсутні	Відповідає
Стійкість до шумів	Мінімальний вплив зовнішніх факторів	Підтверджено експериментально	Відповідає

Результати показують, що отримані значення наближаються до рівномірного розподілу, і що в певних інтервалах не спостерігається значних концентрацій. Це підтверджується статистичними тестами, в яких отримані значення знаходяться в допустимих межах. Високі p-значення вказують на те, що гіпотезу про рівномірний розподіл не можна відхилити.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Крім того, було розраховано ентропію згенерованих послідовностей. Результати показують, що вона знаходиться близько до теоретичного максимуму, що вказує на високий ступінь невизначеності та непередбачуваності. Це важливий критерій для застосувань у криптографії, де навіть невеликі відхилення можуть призвести до вразливостей.

Також були проведені тести випадковості, їх результати представлені у таблиці 3.

Автокореляційний аналіз показує, що згенеровані значення не мають суттєвих залежностей. Кореляційні функції коливаються навколо нуля, що означає, що послідовні значення є статистично незалежними. Це підтверджує, що система не вводить прихованих детермінованих структур під час обробки.

Крім того, було проведено додаткові випробування для оцінки стійкості системи за різних умов. Це включало вивчення впливу коливань температури, коливань напруги та зовнішніх перешкод. Результати показують, що система продовжує стабільно функціонувати, а якість згенерованих даних мінімально погіршується.

Поєднання експериментальних результатів та теоретичного аналізу підтверджує, що розроблена система підходить для застосувань, де потрібен високий ступінь надійності. Інтеграція кількох каналів детектування, обробки аналогових сигналів та методів цифрової корекції призводить до створення надійного рішення, яке може витримувати зовнішні впливи та внутрішні коливання.

Таблиця 3

Узагальнення результатів тестування випадковості

Метод тестування	Мета тесту	Результат	Інтерпретація
χ^2-тест	Перевірка рівномірності	$p = 0{,}77$	Розподіл рівномірний
Колмогоров–Смирнов	Відповідність теоретичному розподілу	$p = 0{,}166$	Відхилення відсутні
Аналіз останньої цифри	Виявлення локальних перекосів	$p = 0{,}8019$	Рівномірність підтверджена
Автокореляція	Перевірка залежностей	≈ 0	Незалежність значень
Стиснення	Виявлення закономірностей	Не стискається	Випадковість підтверджена

Підсумовуючи, технічна реалізація системи успішно демонструє, що квантові джерела шуму можуть бути ефективно використані для генерації випадкових чисел з високою ентропією. Розроблена архітектура поєднує простоту апаратного забезпечення з передовими методами обробки, що призводить до створення системи, яка є одночасно ефективною та надійною. Ці характеристики роблять її особливо придатною для використання в сучасних криптографічних застосуваннях та інших областях, де якість випадковості має вирішальне значення [12].

Висновки

У цьому дослідженні було розроблено інтегрований підхід до генерації випадкових чисел на основі фізичних процесів з внутрішньо ймовірнісним характером. Запропонований метод відрізняється від традиційних рішень тим, що не спирається на детерміновані алгоритми чи класичні джерела, а натомість використовує фундаментальні властивості квантових явищ. Це досягає рівня непередбачуваності, який неможливо відтворити чи передбачити в рамках класичних обчислювальних моделей.

Аналіз існуючих підходів показав, що як псевдовипадкові, так і звичайні генератори мають обмеження. У першому випадку згенерована випадковість зрештою простежується до початкового стану, тоді як у другому випадку зовнішні впливи та структурні нестабільності можуть впливати на якість результату. Ці обмеження підкреслюють необхідність альтернативних рішень, заснованих на фізично недетермінованих процесах.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-3 ISSN 2618-0332 (print), 2618-0340 (online)

Реалізація системи, яка використовує флуктуації електричних сигналів, спричинені дискретною природою носіїв заряду, продемонструвала, що такі процеси можна ефективно використовувати як джерело ентропії. Експериментальні результати підтверджують, що згенеровані послідовності демонструють високий ступінь однорідності та незалежності, що є важливим для застосувань у криптографії та інформаційній безпеці.

Важливим результатом дослідження є підтвердження того, що комбінація кількох незалежних джерел ентропії значно підвищує стійкість системи. Завдяки використанню паралельних каналів детектування та відповідному комбінуванню отриманих сигналів, вплив локальних відхилень та зовнішніх збурень мінімізується. Це призводить до більш стабільного та надійного виходу порівняно з системами, які використовують лише одне джерело випадковості.

Крім того, застосування методів постобробки продемонструвало, що будь-які статистичні відхилення в необроблених даних можна ефективно виправити. Це призводить до двійкової послідовності, яка відповідає вимогам рівномірного розподілу та відсутності кореляцій. Цей крок є важливим для забезпечення практичної зручності використання системи, оскільки навіть незначні відхилення можуть негативно вплинути на криптографічні програми.

Експериментальна оцінка системи підтвердила, що згенеровані дані відповідають загальним статистичним критеріям випадковості. Розраховані значення ентропії наближаються до теоретичного максимуму, що вказує на високий ступінь невизначеності у вихідних даних. Крім того, додаткові аналізи показують, що послідовності не мають значних кореляцій, що ще більше підкреслює придатність системи для використання в критично важливих для безпеки застосуваннях.

Ще одним важливим аспектом є практична доцільність запропонованого рішення. Систему можна реалізувати з використанням поширених електронних компонентів та інтегрувати в існуючі цифрові інфраструктури. Це робить її придатною не лише для дослідницьких цілей, але й для застосування в реальних середовищах, таких як системи безпеки, розподілені мережі та вбудовані системи.

Гнучкість архітектури дозволяє адаптувати систему до різних вимог та застосувань. Такі параметри, як частота дискретизації, обробка сигналу та постобробка, можуть бути оптимізовані залежно від конкретного контексту. Це відкриває можливості для подальшого розвитку та розширення запропонованого методу.

На завершення можна зробити висновок, що використання фізично обґрунтованих джерел ентропії в поєднанні з відповідними методами обробки є перспективним напрямком розробки надійних генераторів випадкових чисел. Результати цього дослідження демонструють, що такий підхід є не лише теоретично обґрунтованим, але й практично здійсненним та ефективним.

Запропоноване рішення, таким чином, сприяє подальшому розвитку безпечних та надійних криптографічних систем. З огляду на постійний технологічний прогрес та зростаючі вимоги в галузі інформаційної безпеки, такий підхід є важливим кроком до перспективних рішень для генерації високоякісних випадкових даних.

Список використаної літератури

1. Horelikova T. O. Enhanced data protection in blockchain: mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies*. 2024. T. 2. P. 40-47. https://doi.org/10.36994/2788-5518-2024-02-08-05
2. Горелікова Т. О. Механізм захисту інформації від підміни та видалення у блокчейн-мережах. *Екзистенційні виклики освіти, науки, безпеки та здоров'я в сучасних умовах: дослідження молодих учених*, м. Одеса, 12 грудня 2024 р. Одеса, 2024. С. 89. https://doi.org/10.32782/2663-5682/2024/41/19
3. Deng L.Y., Kumar N., Lu H. H. S., Yang C. C. Random Number Generators for Computer Simulation and Cyber Security. *Design, Search, Theory, and Application*. Springer. 2025. https://doi.org/10.1007/978-3-031-76722-7

4. Bikos A., Nastou P. E., Petroudis G., Stamatiou Y. C. Random Number Generators. *Principles and Applications*. Cryptography. 2023. T. 7, No 4. P. 54. https://doi.org/10.3390/cryptography7040054
5. Lugrin T. Random Number Generator // Mulder V., Mermoud A., Lenders V., Tellenbach B. (Eds.). Trends in Data Protection and Encryption Technologies. Cham : Springer, 2023. P. 31–34. https://doi.org/10.1007/978-3-031-33386-6
6. Ravichandran H., Sen D., Wali A., Schranghamer T. F., Trainor N., Ray B., Das S. A Peripheral-Free True Random Number Generator Based on Nanoscale Phenomena. *ACS Nano*. 2023. T. 17, No 17. P. 16817. https://doi.org/10.1021/acsnano.3c03581
7. Johnston D. Random Number Generators – Principles and Practices: A Guide for Engineers and Programmers. Berlin: Walter de Gruyter. 2018. https://doi.org/10.1515/9781501506062
8. Kollmitzer C., Schauer S., Rass S., Rainer B. Quantum Random Number Generation: Theory and Practice. Springer. 2020. https://doi.org/10.1007/978-3-319-72596-3
9. Horelikova T., Choporova O., Choporov S. Blockchain as a tool for protecting medical data in artificial intelligence systems. *Artificial Intelligence*. 2025. T. 4. P. 124–131. https://doi.org/10.15407/jai2025.04.124
10. Orszag M. Quantum Optics: Including Noise Reduction, Trapped Ions, Quantum Trajectories, and Decoherence. 4th ed. Springer. 2024. https://doi.org/10.1007/978-3-031-54853-6
11. Cenzer D., Porter C. P. Randomness Extraction in Computability Theory. *Computability*. 2023. T. 12, No 1. P. 1. https://doi.org/10.3233/COM-210343
12. Khrennikov A., Svozil K. (Eds.). Quantum Probability and Randomness. Basel: MDPI Books. 2019. https://doi.org/10.3390/books978-3-03897-715-5

References

1. Horelikova, T. O. (2024). Enhanced data protection in blockchain: mitigating tampering and deletion through randomized checkpoints. *Infocommunication and Computer Technologies*, 2, 40–47. https://doi.org/10.36994/2788-5518-2024-02-08-05 [in English].
2. Horelikova, T. O. (2024). Mekhanizm zakhystu informatsii vid pidminy ta vydalennia u blokcheinmerezhakh [Mechanism for protecting information from substitution and deletion in blockchain networks], Ekzystentsiini vyklyky osvity, nauky, bezpeky ta zdorovia v suchasnykh umovakh: doslidzhennia molodykh uchenykh, materialy Vseukrainskoi naukovo-praktychnoi konferentsii [Existential challenges of education, science, security and health in modern conditions: Research by young scientists, Proceedings of the All-Ukrainian Scientific and Practical Conference], Odesa, December 12, 2024. https://doi.org/10.32782/2663-5682/2024/41/19 [in Ukrainian].
3. Deng, L.Y., Kumar, N., Lu, H.H.S., & Yang, C.C. (2025). Random Number Generators for Computer Simulation and Cyber Security. *Design, Search, Theory, and Application. Springer*. https://doi.org/10.1007/978-3-031-76722-7 [in English].
4. Bikos, A., Nastou, P.E., Petroudis, G., & Stamatiou, Y.C. (2023). Random Number Generators. *Principles and Applications*, *Cryptography*, 7(4), 54. https://doi.org/10.3390/cryptography7040054 [in English].
5. Lugrin, T. (2023). Random Number Generator. In: Mulder, V., Mermoud, A., Lenders, V., & Tellenbach, B. (Eds.). Trends in Data Protection and Encryption Technologies. Cham : Springer. https://doi.org/10.1007/978-3-031-33386-6 [in English].
6. Ravichandran, H., Sen, D., Wali, A., Schranghamer, T. F., Trainor, N., Ray, B., & Das, S. (2023). A Peripheral-Free True Random Number Generator Based on Nanoscale Phenomena. *ACS Nano*, 17(17), 16817. https://doi.org/10.1021/acsnano.3c03581 [in English].
7. Johnston, D. (2018). Random Number Generators – Principles and Practices: A Guide for Engineers and Programmers. Berlin: Walter de Gruyter. https://doi.org/10.1515/9781501506062 [in English].

8. Kollmitzer, C., Schauer, S., Rass, S., & Rainer, B. (2020). Quantum Random Number Generation: Theory and Practice. Springer. https://doi.org/10.1007/978-3-319-72596-3 [in English].
9. Horelikova, T., Choporova, O., & Choporov, S. (2025). Blockchain as a Tool for Protecting Medical Data in Artificial Intelligence Systems. *Artificial Intelligence*, 4, 124–131. https://doi.org/10.15407/jai2025.04.124 [in English].
10. Orszag, M. (2024). Quantum Optics: Including Noise Reduction, Trapped Ions, Quantum Trajectories, and Decoherence (4th ed.). Springer. https://doi.org/10.1007/978-3-031-54853-6 [in English].
11. Cenzer, D., & Porter, C.P. (2023). Randomness Extraction in Computability Theory. Computability, 12(1), 1. https://doi.org/10.3233/COM-210343 [in English].
12. Khrennikov, A., & Svozil, K. (Eds.). (2019). Quantum Probability and Randomness. Basel: MDPI Books. https://doi.org/10.3390/books978-3-03897-715-5 [in English].

Горелікова Тетяна Олексіївна – здобувач вищої освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю «Комп'ютерні науки» Запорізького національного університету. E-mail: uyxkdyc@gmail.com, ORCID: 0009-0001-9098-4618.

Чопорова Оксана Володимирівна – доктор філософії зі спеціальності «Комп'ютерні науки», доцент кафедри комп'ютерних наук Київського національного економічного університету імені Вадима Гетьмана. E-mail: o.choporova@gmail.com, ORCID: 0000-0003-3167-7869.

Horelikova Tetiana Oleksiivna – Postgraduate Student in Computer Science of the Zaporizhzhia National University. E-mail: uyxkdyc@gmail.com, ORCID: 0009-0001-9098-4618.

Choporova Oksana Volodymyrivna – PhD in Computer Science, Associate Professor at the Department of Computer Science of the Kyiv National Economic University named after Vadym Hetman. E-mail: o.choporova@gmail.com, ORCID: 0000-0003-3167-7869.

Дата першого надходження статті до видання: 30.03.2026
Дата прийняття статті до друку після рецензування: 13.05.2026
Дата публікації (оприлюднення) статті: 01.07.2026