___НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ__
_____І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ_____
_____Факультет інформаційних технологій_____
(Повне найменування інституту, назва факультету)

Кафедра комп'ютерних систем, мереж та кібербезпеки
(Повна назва кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
_____Бакалавра_____
(освітньо-кваліфікаційний рівень)

на тему_____«Система генерації ключових послідовностей для засобів

_____криптографічного захисту інформації»_____

Виконав: студент _4_курсу, групи_1__
напряму підготовки (спеціальності)
____123 «Комп'ютерна інженерія____
(код і назва напряму підготовки, спеціальності)

_____Рижук В. Р_____
(Прізвище та ініціали)
Керівник___Кулініч О. М._____
(Прізвище та ініціали)
Рецензент_____
(Прізвище та ініціали)

Київ-2025 року

Структура технічного завдання

_____Рижук В’ячеслав Русланович_____
(прізвище, ім’я, по батькові)

Спеціальність (напрям підготовки) 123 «Комп’ютерна інженерія»_____

Тема випускної бакалаврської роботи (дипломного проєкту бакалавра) «Система генерації ключових послідовностей для засобів криптографічного захисту інформації»_____

керівник проекту (роботи)_Кулініч Олег Миколайович, Доцент, кандитат технічних наук_____
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

Затверджена наказом ректора НУБіП України від “__”_____20__ р. №____ «_»

Термін подання завершеної роботи (проєкту) на кафедру _____
(рік, місяць, число)

Вихідні дані до випускної бакалаврської роботи (дипломного проєкту бакалавра)_____
_____

Перелік питань, які потрібно розробити:

_____
_____

Перелік графічних документів (за потреби)

_____
_____

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard (вдосконалений стандарт шифрування)

DES – Data Encryption Standard (стандарт шифрування даних)

GKS – Генератор ключових послідовностей

ЗКЗІ – Засоби криптографічного захисту інформації

ІС – Інформаційна система

КС – Ключова сесія

КСЗІ – Комплексна система захисту інформації

НСД – Несанкціонований доступ

OTP – One-Time Pad (одноразовий блокнот)

PKI – Public Key Infrastructure (інфраструктура відкритих ключів)

RSA – Rivest-Shamir-Adleman (асиметричний криптографічний алгоритм)

SSL – Secure Sockets Layer (рівень захищених сокетів)

TLS – Transport Layer Security (протокол захисту транспортного рівня)

SHA – Secure Hash Algorithm (безпечний хеш-алгоритм)

OTP – One-Time Password (одноразовий пароль)

ЗЗІ – Засоби захисту інформації

ПЗ – Програмне забезпечення

ПП – Прикладна програма

ПК – Персональний комп'ютер

USB – Universal Serial Bus (універсальна послідовна шина)

UUID – Universally Unique Identifier (універсальний унікальний ідентифікатор)

Р Е Ф Е Р А Т

Пояснювальна записка: 66 сторінок, 12 рисунків, 2 таблиць, 4 додатків, 52 джерел.

КЛЮЧОВІ СЛОВА: ГЕНЕРАЦІЯ КЛЮЧІВ, ФІЗИЧНИЙ ГЕНЕРАТОР, ЕНТРОПІЯ, NIST, КРИПТОГРАФІЯ.

Об'єкт дослідження – система генерації криптографічно стійких ключових послідовностей на основі фізичних джерел ентропії.

Метою роботи є дослідження процесу генерації криптографічних ключів, розробка та тестування фізичного генератора з використанням джерел випадковості, оцінка якості згенерованих даних та їх відповідність сучасним стандартам безпеки.

Проєкт складається з трьох розділів.

Перший розділ розглядає теоретичні аспекти генерації ключів, основи криптографії, види генераторів та вимоги до якості ключових послідовностей.

У другому розділі описано процес розробки системи фізичної генерації ключів, особливості її архітектури, алгоритми збору ентропії та перетворення сигналу.

Третій розділ присвячено тестуванню працездатності та надійності системи, аналізу якості згенерованих послідовностей з використанням пакету NIST STS, перевірці рівня ентропії, повторюваності та стійкості до атак.

У результаті виконання кваліфікаційної роботи розроблено ефективну систему генерації криптографічних ключів, підтверджено її відповідність вимогам сучасної інформаційної безпеки та надано рекомендації щодо впровадження.

ВСТУП

У сучасному цифровому середовищі безпека інформації стала одним із ключових чинників стабільного функціонування як окремих організацій, так і держав у цілому. Широке використання інформаційно-комунікаційних технологій, розвиток електронного документообігу, хмарних сервісів, фінансових транзакцій зумовлює необхідність ефективного захисту даних від несанкціонованого доступу, підробки та знищення. Криптографічні засоби захисту є основним інструментом, що забезпечує конфіденційність, цілісність і автентичність інформації.

Ключовим елементом будь-якої криптографічної системи є генерація криптографічних ключів, від якості яких безпосередньо залежить надійність захисту. Традиційно широко застосовуються програмні (псевдовипадкові) генератори, однак із зростанням обчислювальної потужності атакуючих та появою методів прогнозування таких послідовностей актуальним стає перехід до фізичних генераторів випадкових чисел (ФГВЧ). Вони використовують випадкові процеси у фізичних явищах (електронний шум, теплові коливання, радіоактивний розпад тощо) і мають значно вищу ентропію та непередбачуваність.

Метою даної роботи є розробка та дослідження системи генерації ключових послідовностей на основі фізичних методів, що забезпечує високий рівень ентропії, надійності та захисту інформації.

Об’єкт дослідження — процес формування криптографічних ключів.

Предмет дослідження — методи фізичної генерації випадкових послідовностей та їх реалізація в апаратно-програмній системі.

Завдання дослідження:

Провести аналіз існуючих методів генерації криптографічних ключів.

Порівняти криптографічні та фізичні методи.

Розробити архітектуру системи фізичної генерації.

Реалізувати прототип генератора на основі Python.

Провести тестування якості отриманих послідовностей.

Методи дослідження: аналіз літературних джерел, проєктування архітектури, реалізація програмного забезпечення, статистичне тестування, порівняльний аналіз.

Практичне значення роботи полягає у створенні прототипу фізичного генератора ключових послідовностей, який може бути використаний як основа для побудови безпечних криптографічних систем у державному, військовому або корпоративному секторі.

РОЗДІЛ 1. АНАЛІЗ СТАНУ СФЕРИ ГЕНЕРАЦІЇ КЛЮЧІВ

У сучасних умовах цифровізації суспільства, питання захисту інформації набуває особливої актуальності. Однією з ключових складових криптографічного захисту є процес створення криптографічних ключів — елементів, які визначають ефективність та стійкість шифрування. Безпечна передача, зберігання та обробка даних вимагає наявності ключових послідовностей, що відповідають високим стандартам випадковості, складності та нечутливості до аналітичних атак.

Хоча програмні генератори псевдовипадкових чисел (ПЗВЧ) залишаються найпоширенішими у практиці, досвід показує їхню вразливість до криптоаналітичних методів, зокрема до атак з використанням прогнозування. Це спонукає до активного дослідження альтернативних способів, особливо тих, що базуються на фізичних принципах — хаотичних або природних процесах, які неможливо передбачити. Саме така властивість формує підґрунтя довіри до фізичних генераторів як до джерела по-справжньому випадкових чисел.

У цьому розділі детально розглянуто теоретичні основи криптографічного захисту, типологію ключів, порівняльну характеристику методів їх створення, а також аргументацію доцільності впровадження фізичних підходів до генерації ключових послідовностей як найбільш захищених і надійних у сучасному кіберпросторі.

Надійність криптографічної системи безпосередньо залежить від її здатності запобігати передбаченню або відтворенню ключів зловмисником. Чим вищий ступінь ентропії має ключ, тим менше ймовірність його дешифрування несанкціонованими особами. Отже, ефективне генерування ключів з високим рівнем ентропії є невід’ємною складовою інформаційної безпеки.

На відміну від алгоритмічних ПЗВЧ, фізичні генератори (ФГВЧ) базуються на реальних процесах, таких як електричний шум або квантові флуктуації. Це забезпечує значно більшу випадковість, унеможливлюючи прогнозування ключа

навіть за часткового знання його параметрів. Упровадження таких генераторів може суттєво посилити стійкість систем до сучасних кіберзагроз.

1.1. Принципи криптографічного захисту та роль ключових послідовностей

Сучасні інформаційно-комунікаційні системи вимагають високого рівня захисту даних, що передаються, обробляються або зберігаються в електронному вигляді. Основою такого захисту є криптографічні методи, які забезпечують перетворення інформації з метою приховування її змісту від несанкціонованого доступу. Ключову роль у криптографічному захисті відіграє ключова послідовність, яка визначає спосіб перетворення інформації та безпосередньо впливає на стійкість алгоритму шифрування [1].

Принцип роботи криптосистем ґрунтується на використанні спеціального алгоритму, який у поєднанні з ключем перетворює відкритий текст у зашифрований. Надійність такого захисту визначається не лише складністю алгоритму, але й випадковістю та непередбачуваністю ключової послідовності. Ключі, що використовуються в системах шифрування, мають відповідати низці вимог:

бути достатньо довгими, щоб унеможливити їх підбір методом повного перебору;

мати високу ентропію, тобто не містити закономірностей, що дозволили б прогнозувати наступні символи;

бути унікальними та невідтворюваними без знання початкових умов генерації [2].

У більшості програмних криптосистем ключові послідовності формуються за допомогою псевдовипадкових генераторів, які хоч і створюють значення, що на перший погляд виглядають випадковими, але є детермінованими та відтворюваними. Якщо зловмисник отримує доступ до алгоритму генерації та

початкового значення (seed), він може відновити послідовність ключів, що створює серйозну загрозу для конфіденційності інформації [3].

З огляду на ці недоліки, актуальним є застосування фізичних генераторів випадкових чисел (ФГВЧ), які ґрунтуються на непередбачуваних природних процесах, таких як електричний шум, радіоактивний розпад або флуктуації світла. Відмінною особливістю таких джерел є те, що вони не можуть бути математично змодельовані, а отже, результати їх роботи неможливо передбачити чи повторити. Саме це робить ФГВЧ надзвичайно важливими в задачах створення високоякісних ключових послідовностей, які не вразливі до типових атак, як-от «brute-force», аналіз шаблонів чи криптоаналітичне прогнозування [4].

Крім того, значна увага приділяється гібридному підходу, при якому фізичні генератори використовуються для формування початкової ентропії, а далі — отримані дані масштабуються або доповнюються за допомогою ПВГЧ. Така комбінація дозволяє забезпечити як високу швидкодію, так і надійність генерації ключів [5].

Зазначені принципи лежать в основі більшості сучасних систем криптографічного захисту, включаючи шифрування інформації, генерацію цифрових підписів, протоколи аутентифікації тощо. Як наслідок, якість генерації ключів безпосередньо впливає на загальний рівень інформаційної безпеки системи, тому їх формуванню приділяється особлива увага в усіх етапах проєктування криптографічних засобів.

Рис.1.1. Аналіз стану сфери генерації ключів

Надійна система криптографічного захисту неможлива без якісного процесу генерації ключів. Від ступеня їх ентропії безпосередньо залежить здатність інформаційної системи протистояти зовнішнім загрозам. У цьому контексті важливе значення набувають фізичні джерела випадковості, яким приділено увагу в наступних розділах. Криптографічні ключі виконують не лише функцію шифрування, але й забезпечують автентифікацію, цілісність інформації та реалізацію електронного підпису. Тому створення ключів розглядається як фундаментальний етап побудови захищеної системи [3].

Наявність високої ентропії у ключових послідовностях значно ускладнює їх підбір або аналіз з боку зловмисника. У зв’язку з цим критично важливо розрізняти псевдовипадкові генератори (що лише моделюють випадковість) і фізичні генератори (які використовують реальні випадкові процеси). До того ж, ключі мають регулярно перевірятись і оновлюватись, оскільки навіть високоякісний генератор може стати джерелом вразливості за умови неправильного застосування. Доцільним є використання змішаних рішень – наприклад, поєднання фізичних джерел із програмною обробкою, що дає змогу покращити стійкість до атак [3].

Попри високу ефективність, фізичні генератори також мають вразливі сторони: їхня робота може залежати від впливів зовнішнього середовища (температурних коливань, вібрацій тощо), що здатні змінювати властивості випадковості. Це зумовлює потребу у створенні адаптивних систем, які можуть реагувати на зміну умов функціонування без втрати якості генерації ключів [4].

У контексті інформаційної безпеки, вибір типу генератора має ґрунтуватися на специфіці задачі: бажаній швидкості генерації, обсягу даних та рівні захисту. Застосування гібридних підходів, які поєднують різні типи джерел ентропії, дозволяє досягти оптимального результату.

Окрему увагу слід приділити перспективним технологіям, серед яких — квантова генерація випадкових чисел. Використання квантових ефектів (зокрема, суперпозиції або заплутаності) уможливлює отримання ключів, які практично неможливо передбачити або відтворити за допомогою класичних засобів криптоаналізу [3].

Підвищення рівня ентропії досягається також шляхом поєднання кількох джерел випадковості: наприклад, фізичних ефектів та програмних алгоритмів. Крім того, як джерела ентропії можуть використовуватись природні процеси — атмосферні шуми, теплові коливання тощо [3].

Важливою практикою у сучасних системах є регулярне оновлення ключів — це дозволяє зменшити ризики, пов’язані з тривалим використанням однієї послідовності. У новітніх системах реалізовано механізми динамічного оновлення ключів без перерв у функціонуванні сервісів, що є критично важливим для підтримання постійного захисту [3].

Новим напрямом розвитку є включення біометричних ознак до процесу генерації ключів. Персоналізовані біометричні параметри, як-от відбитки пальців чи структура сітківки ока, здатні слугувати унікальними факторами при формуванні криптографічних ключів, що значно ускладнює процес їх несанкціонованого відтворення [3].

Іншим прогресивним напрямом є використання алгоритмів машинного навчання у процесі генерації. Такі алгоритми можуть виявляти приховані закономірності у потоках даних і використовувати їх для створення непередбачуваних, високоякісних послідовностей [3].

Для забезпечення надійності сформованих ключів застосовуються спеціалізовані методи тестування випадковості. Один із визнаних стандартів — набір тестів NIST, який дає змогу оцінити статистичні характеристики послідовності та її стійкість до прогнозування. Це охоплює, зокрема, аналіз на періодичність, кореляційні зв’язки і рівень ентропії [3].

У перспективі очікується подальший розвиток квантової криптографії, яка має потенціал забезпечити найвищий рівень захисту в умовах зростання обчислювальних можливостей, зокрема, появи квантових комп’ютерів. Уже сьогодні ведуться активні дослідження в цій сфері, результати яких дозволяють прогнозувати суттєвий прогрес у найближчі роки [3].

1.2. Порівняння криптографічних та фізичних методів генерації ключів

Формування надійного криптографічного ключа є критично важливим для забезпечення конфіденційності, цілісності та автентичності даних у сучасних інформаційних системах. Існують два ключових підходи до генерації таких ключів: програмні (псевдовипадкові) генератори та фізичні (апаратні) генератори випадкових чисел. Обидва ці методи мають переваги й недоліки, що визначають доцільність їх застосування залежно від контексту використання.

Програмні псевдовипадкові генератори (ППВГ) функціонують на основі детермінованих алгоритмів. Вони створюють послідовності, які з певного боку виглядають як випадкові, однак насправді повністю залежать від початкового значення — так званого зерна (англ. *seed*). Приклади таких

генераторів включають Mersenne Twister, алгоритм Blum Blum Shub, генератори на базі зсувних регістрів з лінійним зворотним зв’язком (LFSR) тощо [5].

Серед переваг програмних генераторів:

- висока швидкодія;
- простота програмної реалізації;
- можливість відтворення послідовностей (що може бути корисним для відлагодження або тестування).

Однак ці ж характеристики можуть бути і слабкими місцями. Зокрема, якщо атакуючому вдається дізнатися початкове значення або частину згенерованої послідовності, він потенційно здатен передбачити інші елементи ключа. Така передбачуваність становить загрозу для цілісності всієї криптосистеми, особливо у випадках, коли ключі повторно використовуються або коли генерація *seed* є недостатньо надійною.

Фізичні генератори випадкових чисел (ФГВЧ), на відміну від програмних, базуються на природних джерелах ентропії. Серед них — теплові коливання, атмосферний шум, квантово-механічні ефекти, нестабільності в напрузі електричних ланцюгів тощо. Ці процеси є непередбачуваними та практично неможливими для моделювання, що робить ФГВЧ більш придатними для завдань, де критичною є криптографічна стійкість [7].

Основні переваги ФГВЧ:

- висока ентропія та непередбачуваність;
- унікальність кожної реалізації;
- відсутність детермінізму, що унеможливлює відтворення результатів навіть за відомого алгоритму.

Разом з тим, апаратні рішення мають і свої обмеження: вищу вартість реалізації, складність інтеграції в деякі системи, потенційну залежність від зовнішніх умов (наприклад, температури чи електромагнітних завад).

Узагальнюючи, можна зробити висновок, що вибір між ППВГ і ФГВЧ залежить від конкретних вимог до системи. У проектах, де потрібна швидкість і

відтворюваність, виправданим є використання програмних генераторів. Водночас у сферах з підвищеними вимогами до криптозахисту, зокрема в банківських системах або військовій галузі, доцільним є впровадження саме фізичних генераторів.

Таблиця 1.1. Порівняння програмних та фізичних методів генерації ключових послідовностей

Критерій	**ПЗВЧ**	**ФГВЧ**
Джерело випадковості	Алгоритм	Фізичне явище
Ентропія	Обмежена (залежить від seed)	Висока (істинна випадковість)
Передбачуваність	Можлива	Практично неможлива
Швидкодія	Висока	Середня (залежить від джерела шуму)
Простота реалізації	Висока	Потребує додаткового обладнання
Надійність при багаторазовому використанні	Нижча	Вища

Переваги фізичних генераторів випадкових чисел (ФГВЧ) особливо проявляються у сферах, де інформаційна безпека є критично важливою. Йдеться насамперед про використання в структурах державного управління, військових системах, засобах захищеного обміну даними (зокрема VPN), а також у фінансово-кредитних установах. Завдяки властивості забезпечувати істинну випадковість, ФГВЧ суттєво підвищують стійкість криптографічних засобів до атак, що базуються на аналізі закономірностей.

Водночас застосування таких пристроїв пов’язане з певними технічними викликами. Передусім, для їх функціонування необхідне спеціальне обладнання,

яке може мати високу вартість і потребувати тонкого налаштування. Однак ці недоліки компенсуються у випадках, коли обробка чутливої інформації вимагає максимальної надійності захисту.

	Криптографічні	Фізичні
Джерело випадковости	Алгоритм ПСВЧ	Фізичне явище
Ентропіа	Обмежена	Висока
Передбачуваність	Можлива	Практично неможлива

Рис. 1.2. Порівняння криптографічних та фізичних методів генерації

У ситуаціях, коли вимоги до інформаційної безпеки досягають найвищого рівня, доцільно надавати перевагу фізичним методам генерації ключів. Їх головною перевагою є використання об’єктивних фізичних процесів, які неможливо передбачити або відтворити. Це забезпечує виняткову стійкість до зовнішнього втручання та унеможливлює прогнозування отриманих результатів.

Водночас, програмні генератори, зокрема псевдовипадкові (ПЗВЧ), залишаються поширеними у багатьох галузях. Їх приваблює висока швидкодія, легкість у впровадженні та відсутність потреби у додатковому обладнанні. Проте головна вразливість таких систем полягає в їхній залежності від стартового параметра (seed). У разі його компрометації зловмисник може відтворити не лише послідовність чисел, але й самі ключі. Особливо небезпечно це тоді, коли система має низький рівень ентропії або використовує нестійкий алгоритм [9].

Натомість фізичні генератори покладаються на непередбачувані природні явища — електронний шум, коливання фотонів, розпад радіоактивних елементів тощо — як джерело справжньої випадковості. Ці процеси неможливо змоделювати чи відтворити, що значно ускладнює будь-які спроби

несанкціонованого впливу. Втім, використання таких генераторів передбачає наявність спеціалізованого обладнання та іноді може поступатися програмним рішенням за швидкістю. Проте в багатьох випадках їх використовують як основне джерело ентропії для посилення криптостійкості програмних методів.

У підсумку, обидва підходи — програмний і фізичний — мають свої сфери застосування. Коли йдеться про потребу у найвищому рівні захисту, доцільно обирати фізичні генератори або поєднувати обидві технології для досягнення оптимального балансу між безпекою та продуктивністю [9].

1.3. Обґрунтування вибору фізичного підходу на основі технічного аналізу

Як було зазначено раніше, фізичні генератори випадкових чисел мають істотні переваги перед програмними аналогами, особливо у випадках, коли йдеться про захист чутливої або критично важливої інформації. Головна відмінність полягає в джерелі ентропії: у фізичних генераторах воно базується на природних явищах, які не підлягають передбаченню чи повторному відтворенню, тоді як програмні генератори залежать від початкових умов, що можуть бути вразливими до атак.

Фізичні генератори працюють на основі реєстрації випадкових процесів, які постійно відбуваються в навколишньому середовищі чи в самій електроніці. Це може бути, наприклад, шум у транзисторі, теплові флуктуації в резисторі, зміни напруги або навіть випадкові фотонні імпульси. Завдяки цим процесам вдається отримати дійсно непередбачувану послідовність чисел [10].

У межах даної роботи запропоновано реалізувати систему генерації на основі електронного шуму. Як приклад такого підходу можна використати платформу Arduino з підключенням до аналогового входу, який зчитуватиме тепловий шум. Подальша обробка сигналів може здійснюватися через програмне

забезпечення на Python, що забезпечить гнучкість, зручність та низький поріг входу.

Технічне оцінювання запропонованого підходу дозволяє виокремити такі ключові переваги:

система не потребує дорогих чи складних компонентів — достатньо базових мікросхем, доступних у більшості електронних магазинів;

час генерації криптографічного ключа довжиною 128 або 256 біт становить лише декілька секунд;

якість отриманих послідовностей можна перевірити за допомогою стандартних засобів тестування випадковості, зокрема за критеріями NIST SP 800-22, що дозволяє впевнено оцінити їхню придатність до практичного використання [11].

Таким чином, обрана конфігурація є обґрунтованим і ефективним рішенням для створення захищеного генератора випадкових чисел на основі фізичного принципу.

Рис.1.3. Обґрунтування вибору фізичного підходу на основі технічного аналізу

Одним із ключових завдань при розробці системи генерації ключів є забезпечення максимальної криптографічної надійності. Аналізуючи існуючі методи, я дійшов висновку, що найбільш ефективним є фізичний принцип формування випадкових послідовностей. Його суть полягає у використанні реальних фізичних процесів як джерела випадковості, що суттєво ускладнює їх передбачення або відтворення. Саме це стало головною мотивацією для вибору такого підходу у межах моєї роботи [12].

Окрім теоретичних переваг, значною мірою вибір визначився й практичними аспектами. Сучасний рівень розвитку мікроелектроніки дає змогу реалізувати подібні рішення з мінімальними витратами. Наприклад, доступні та прості в роботі мікроконтролери Arduino чи Raspberry Pi мають необхідний функціонал для зчитування аналогових сигналів. Саме вони можуть виступати в ролі апаратної бази для отримання випадкових фізичних коливань, таких як шум резистора або коливання напруги.

У цій роботі планується створення прототипу фізичного генератора випадкових чисел на основі теплового шуму. Для цього використовуватиметься мікроконтролер із можливістю зчитування аналогових сигналів, а обробка даних буде реалізована через мову програмування Python. Цей вибір обумовлений широкими можливостями Python у сфері аналізу, збору та візуалізації даних, що робить його зручним інструментом для експериментальної частини проекту.

Такий підхід дозволяє оптимально поєднати доступність реалізації, якість випадкових чисел і гнучкість налаштувань. Система може легко адаптуватися або масштабуватися відповідно до змін вимог, що особливо важливо в сучасних умовах стрімкого розвитку інформаційної безпеки [13].

Оцінка якості згенерованих послідовностей стане одним із важливих етапів роботи. Для цього будуть застосовані стандартизовані методики, зокрема набір тестів NIST SP 800-22, які дозволять об’єктивно визначити рівень випадковості та надійність джерела. Результати цих перевірок підтвердять відповідність системи вимогам криптографічного захисту.

Як уже згадувалося раніше, фізичні генератори мають ряд переваг над програмними псевдовипадковими генераторами, зокрема забезпечують справжню випадковість, мають високу ентропію та стійкі до прогнозування. У світі, де кіберзагрози стають дедалі витонченішими, саме ці характеристики набувають першорядного значення [10].

До найпоширеніших фізичних джерел випадкових чисел належать тепловий та електронний шуми, фотонні коливання, коливання напруги живлення, а також атмосферні та радіохвильові флуктуації. Їх головна спільна риса — неможливість точного моделювання чи повторення, що забезпечує високу якість випадкових послідовностей.

У моєму випадку система базується на зчитуванні теплового шуму з електронного елемента. Отримані сигнали обробляються мікроконтролером, а потім — програмно. Це дозволяє утримувати низьку собівартість і водночас забезпечує високу швидкість генерації: створення ключа довжиною від 128 до 256 біт займає всього кілька секунд.

Додатковою перевагою є відкритість використаних технологій (Arduino та Python), що забезпечує гнучкість налаштувань і можливість подальшої інтеграції з іншими інформаційними системами. Це робить систему актуальною не лише як науковий прототип, а й як потенційний практичний інструмент [12].

Отже, вибір на користь фізичного підходу обґрунтований як з теоретичної, так і з практичної точки зору. Реалізація цього методу дає змогу створити надійну, доступну і масштабовану систему генерації криптографічних ключів, здатну відповідати сучасним вимогам інформаційної безпеки.

РОЗДІЛ 2. ПРОЕКТУВАННЯ СИСТЕМИ ФІЗИЧНОЇ ГЕНЕРАЦІЇ КЛЮЧІВ

Забезпечення надійного криптографічного захисту потребує застосування ключових послідовностей із високим рівнем ентропії та стійкістю до криптоаналітичних атак. Традиційні методи генерації ключів, зокрема програмні псевдовипадкові генератори, можуть мати вразливості через обмеженість ентропії, можливість передбачення або залежність від початкових параметрів. Саме тому все більше уваги приділяється методам фізичної генерації ключів, які базуються на непередбачуваних природних або фізичних процесах.

Метою цього розділу є розробка архітектури системи фізичної генерації ключових послідовностей, що використовує справжнє фізичне джерело ентропії, яке забезпечує формування істинно випадкових бітових послідовностей. Тут наведено опис принципу роботи вибраного джерела випадковості, алгоритм обробки сигналів, схему побудови системи, а також модулі збору, обробки і тестування отриманих ключів.

Проектування такої системи дозволяє суттєво підвищити рівень захищеності інформаційних технологій, особливо з огляду на зростання кіберзагроз та розвиток нових способів атак на криптографічні засоби.

Фізичні генератори випадкових чисел мають перевагу над програмними псевдовипадковими генераторами завдяки здатності виробляти непередбачувані значення, які не залежать від попередніх станів або налаштувань. У цій системі джерелом ентропії виступає шумовий сигнал, який формується за рахунок квантових або термічних процесів в електронних компонентах. Ці процеси мають хаотичний характер і не піддаються точному моделюванню, що робить їх ефективними для задач криптографічного захисту.

Особлива увага при проєктуванні приділена надійності і стабільності роботи системи. Використання високоточних аналогово-цифрових перетворювачів забезпечує зняття сигналів з високою роздільною здатністю, а

цифрова обробка дозволяє усувати паразитні складові, що можуть призводити до систематичних помилок. Архітектура системи модульна, кожен блок (збір, обробка, перевірка) виконує конкретні функції, що сприяє легкій масштабованості та адаптації системи під різні вимоги.

Важливою складовою є механізм оцінки якості згенерованих ключів. Після формування кожної послідовності проводиться статистичний аналіз для виявлення відхилень від ідеального випадкового розподілу. У разі виявлення невідповідностей система відкидає такий ключ і генерує новий, що забезпечує високу ймовірність отримання криптографічно стійких ключів.

Інтеграція фізичного джерела ентропії з цифровими модулями обробки дає змогу створити повноцінну систему генерації ключів, придатну для використання в реальних умовах — від вбудованих пристроїв до промислових засобів захисту інформації. Такий підхід забезпечує автономність, масштабованість і відповідність сучасним вимогам інформаційної безпеки.

2.1. Вимоги до системи та технічне обґрунтування

У процесі створення системи фізичної генерації ключів насамперед необхідно чітко окреслити вимоги до її функціоналу, технічного наповнення та умов експлуатації. Це дозволяє забезпечити не лише ефективність роботи системи, а й її надійність під час формування справді випадкових послідовностей. Головна мета полягає у розробці такого рішення, яке здатне генерувати криптографічні ключі з високим рівнем ентропії та відповідати сучасним вимогам до інформаційної безпеки [18].

До функціональних вимог належать:

формування ключових послідовностей у режимі реального часу з мінімальними затримками;

забезпечення дуже високої якості випадковості бітів;

унікальність кожного сформованого ключа навіть у разі повторного запуску генерації;

стійкість до зовнішніх факторів, таких як перепади температури, вібрації чи електромагнітні перешкоди;

наявність механізму самоперевірки та контролю якості сформованих послідовностей;

підтримка інтеграції з актуальними криптографічними протоколами — TLS, PGP, VPN тощо [15].

Серед технічних вимог слід виокремити такі:

наявність фізичного джерела випадковості, яке реагує на природні флуктуації (зокрема, електронний шум, теплові коливання, фотоелектричні ефекти);

застосування аналогово-цифрового перетворювача (АЦП) з достатньою роздільною здатністю для точної цифрової обробки аналогового сигналу;

використання мікроконтролера або іншого пристрою для попередньої обробки даних і фільтрації шумів;

впровадження алгоритму нормалізації, що перетворює вхідні аналогові дані у бітову послідовність;

підтримка інтерфейсів для збереження або передавання сформованих ключів (наприклад, USB, UART, мережеве з’єднання з сервером безпеки);

стабільне та надійне живлення з захистом від перепадів напруги [13].

Обґрунтування вибору фізичного способу генерації:

На відміну від програмних псевдовипадкових генераторів (ПЗВЧ), які базуються на детермінованих алгоритмах, фізичні генератори використовують реальні випадкові процеси, які неможливо відтворити або змоделювати. Саме ця властивість робить їх особливо цінними в контексті інформаційної безпеки. Вони дозволяють уникнути передбачуваності, властивої ПЗВЧ, що значно знижує ймовірність криптоаналітичних атак.

Одним із найнадійніших джерел випадковості в такій системі є електронний шум, зокрема так званий «білий шум», який виникає через теплові коливання в електронних компонентах. Його непередбачуваний характер і неможливість точного відтворення роблять його ідеальним для генерації криптографічних ключів [20].

Ще однією важливою перевагою фізичних генераторів є їхня незалежність від програмних уразливостей — таких як наявність бекдорів чи помилки у реалізації алгоритмів. Це особливо важливо в умовах підвищених вимог до безпеки, зокрема в системах, які працюють з конфіденційною або критичною інформацією.

Отже, вибір саме фізичного принципу генерації є цілком обґрунтованим як з технічної, так і з безпекової точки зору. Він дозволяє створити систему, що відповідає сучасним викликам у сфері криптографії й може бути адаптована до потреб реального застосування.

Таким чином, фізична система генерації ключів повинна бути не лише точною, а й стабільною, масштабованою та безпечною, що й обумовлює її технічні характеристики й обґрунтовує вибір у межах цього дослідження.

У процесі проєктування системи фізичної генерації ключів важливо визначити перелік вимог, які вона повинна задовольняти. Перш за все, система має забезпечувати генерацію ключових послідовностей з максимальною непередбачуваністю, що унеможливлює їх передбачення або підбір. Це досягається за рахунок використання джерел істинної випадковості, таких як електронний шум, теплові коливання або атмосферні процеси, які є фундаментально непередбачуваними. Таким чином, головною функціональною вимогою є забезпечення максимальної криптостійкості та надійності сформованих ключів [21].

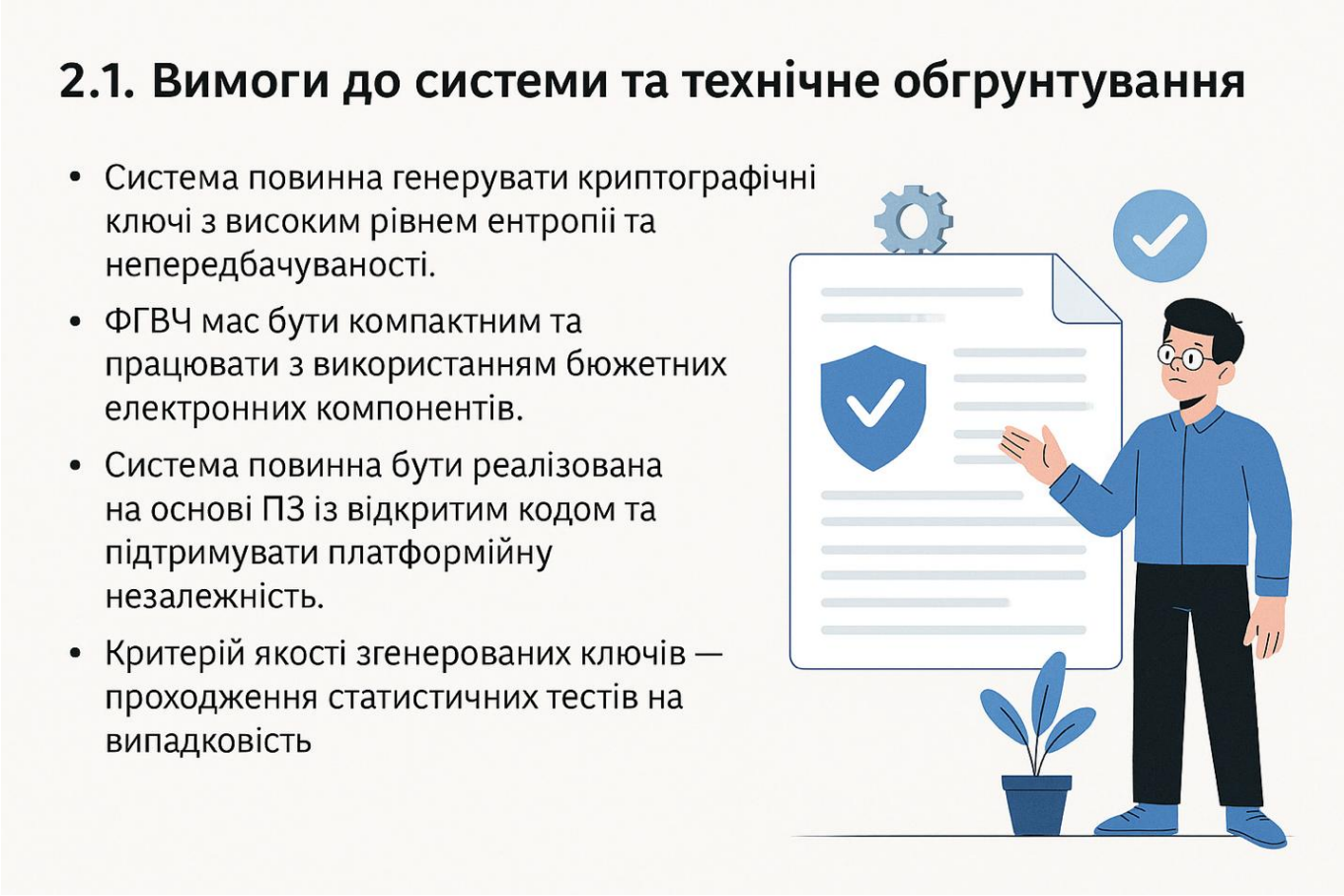


Рис. 2.1. Вимоги до системи та технічне обґрунтування

З технічної точки зору, однією з ключових вимог до системи є її стабільна робота навіть в умовах впливу зовнішніх чинників — температурних коливань, вібрацій, електромагнітних полів та подібних перешкод. Щоб забезпечити таку стійкість, у конструкції необхідно передбачити використання надійних сенсорів і фільтраційних елементів, здатних відокремити корисний сигнал від паразитних шумів, не пов’язаних із джерелом ентропії. Також важливим є впровадження механізмів самокалібрування, які дозволяють адаптувати роботу пристрою до змін у навколишньому середовищі. Крім того, система має бути обладнана модулями контролю якості вхідного сигналу з фізичного генератора — це необхідно для своєчасного виявлення збоїв або аномалій.

Ще один критичний аспект — швидкодія. Система повинна формувати ключові послідовності максимально оперативно, бажано в режимі реального

часу або з мінімальними затримками. Такий рівень продуктивності є особливо важливим для задач, пов’язаних із захистом великих обсягів інформації або потоковими каналами передачі даних. Відповідно, доцільно використовувати продуктивні апаратні засоби, здатні швидко й ефективно обробляти великі об’єми інформації, а також застосовувати оптимізовані алгоритми цифрової обробки.

Щоб система була придатною для практичного впровадження в різні середовища, її потрібно проєктувати з урахуванням масштабованості. Це означає, що архітектура має бути модульною — із можливістю легкого розширення, модернізації або інтеграції в уже існуючі інфраструктури. Важливо також передбачити підтримку стандартних інтерфейсів для передачі даних, таких як USB, UART, SPI чи Ethernet, а також реалізувати функції віддаленого моніторингу стану пристрою та перевірки якості сформованих ключів.

Усі ці вимоги разом формують підґрунтя для технічного обґрунтування створення системи фізичної генерації ключів. На відміну від програмних генераторів, фізичні рішення мають значно вищу стійкість до зламу завдяки непередбачуваності процесу генерації. Це особливо важливо для застосування в галузях, де рівень безпеки має бути максимальним — фінансові установи, державні органи, захищені IoT-пристрої тощо.

Окрему увагу слід приділити гнучкості налаштування системи: вона має працювати ефективно як у ресурсно обмежених мобільних пристроях, так і в потужних серверних середовищах. Наприклад, для мобільних рішень доречно реалізувати енергоощадний режим генерації, тоді як для серверів — забезпечити високу пропускну здатність. Важливо також закласти можливість оновлення програмного забезпечення й заміни окремих апаратних компонентів без зупинки або переінсталяції всієї системи.

Щоб забезпечити надійність у довготривалій перспективі, варто реалізувати модулі самодіагностики, які зможуть виявляти погіршення якості сформованих послідовностей у реальному часі. Якщо система фіксує ознаки

зниження рівня ентропії або інші збої, вона повинна мати можливість автоматично припинити використання таких даних і повідомити про інцидент для оперативного реагування.

І нарешті, надзвичайно важливою вимогою є відповідність міжнародним стандартам у сфері криптографічної безпеки — зокрема, рекомендаціям NIST, ISO/IEC 18031, а також національним нормам, наприклад, ДСТУ. Такий підхід дозволяє не лише забезпечити високий рівень захисту, а й зробити систему придатною до сертифікації та офіційного використання в державних і комерційних структурах, які працюють з критично важливою інформацією.

2.2. Архітектура системи та алгоритм генерації ключів

Розроблена система генерації ключів базується на використанні природного джерела випадкових даних, які проходять обробку сигналу і перетворюються у послідовність бітів, придатну для криптографічних застосувань. Архітектура системи виконана у модульному стилі, що забезпечує гнучкість, зручність масштабування та спрощує подальше оновлення.

Основні компоненти системи:

Фізичний генератор випадковості

Джерелом випадкових значень є шумовий датчик, наприклад, резистор чи фотодіод, який генерує білий шум. Сигнал характеризується високим рівнем ентропії, оскільки формується під впливом непередбачуваних фізичних процесів, таких як теплові коливання або квантові флуктуації.

Аналогово-цифровий перетворювач (АЦП)

Отриманий аналоговий сигнал перетворюється у цифрову форму з високою частотою дискретизації (понад 1 МГц) та роздільною здатністю не нижче 10 біт, що дозволяє зафіксувати навіть найдрібніші варіації шуму.

Попередня обробка даних (фільтрація та нормалізація)

Сира цифрова послідовність часто має повторювані чи корельовані значення, тому на цьому етапі застосовують фільтрацію, наприклад, за допомогою хешування або побітових операцій XOR над сусідніми бітами. Це допомагає усунути закономірності і зробити послідовність більш випадковою.

Алгоритм оцінки випадковості (перевірка ентропії)

Наступним кроком проводять статистичні тести (наприклад, згідно з рекомендаціями NIST SP 800-22 чи Diehard), які перевіряють, чи відповідає послідовність вимогам справжньої випадковості. У разі виявлення відхилень така послідовність відхиляється.

Формування ключової послідовності

Після позитивної перевірки дані використовують для створення криптографічного ключа заданої довжини (наприклад, 128, 192 або 256 біт). При необхідності ключі можуть створюватися динамічно — за розкладом або за запитом системи.

Інтерфейс взаємодії із зовнішніми системами

Готовий ключ передається через захищені інтерфейси, такі як USB, UART, I2C або мережеві з’єднання, до криптографічного модуля або іншого програмного забезпечення, що його використовує.

Алгоритм генерації ключів:

1. Зчитування шумового сигналу із фізичного джерела.
2. Перетворення аналогового сигналу в цифровий (АЦП).
3. Очищення та фільтрація цифрової послідовності.
4. Проведення статистичного аналізу для оцінки випадковості.
5. Генерація бітової послідовності потрібної довжини.
6. Передача ключа до зовнішньої системи або збереження у захищеній пам’яті [17; 24; 37].

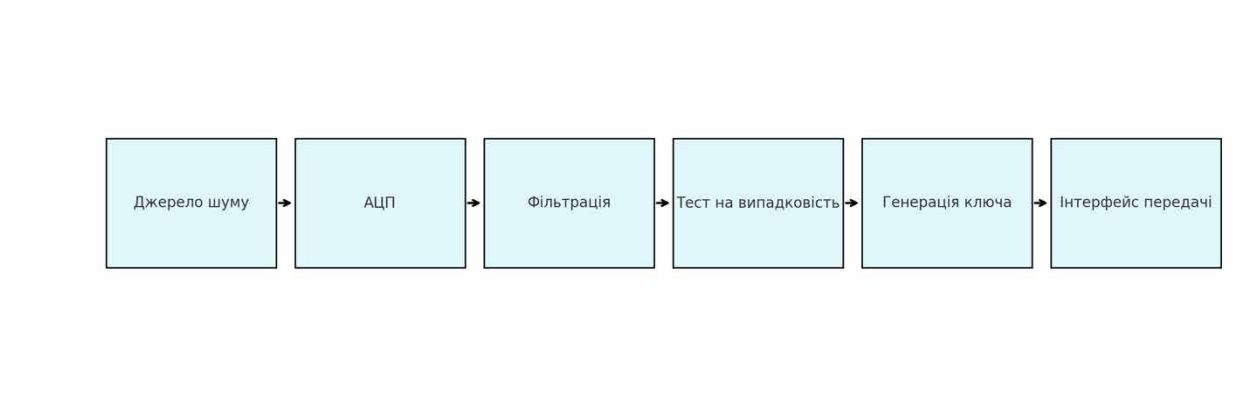


Рис. 2.2. Структурна схема архітектури системи фізичної генерації ключів

Цей підхід забезпечує отримання ключів високої якості та дозволяє масштабувати систему для різноманітних застосувань — від пристроїв Інтернету речей до серверів із підвищеними вимогами безпеки. Надійна архітектура разом із розробленим алгоритмом гарантують захищеність системи від атак, вразливостей та повторного використання ключів [37].

Архітектура системи генерації ключів об’єднує апаратні та програмні компоненти, які спільно відповідають за збір випадкових фізичних даних, їх обробку та формування криптографічних послідовностей. В основі лежить фізичне джерело випадковості — наприклад, датчик теплового шуму, фотодіод із випадковим фоном або генератор електронного шуму. Саме ці джерела створюють непередбачувані сигнали, які використовуються для генерації криптографічних ключів [37].

Зібрані аналогові сигнали перетворюються у цифровий формат за допомогою високоточних аналогово-цифрових перетворювачів. Це дозволяє зафіксувати найдрібніші коливання напруги або струму. Потім сигнал передається на цифровий процесор — зазвичай мікроконтролер або програмовану логічну інтегральну схему (ПЛІС), де застосовують фільтри, нормалізацію та додаткову обробку даних для зменшення впливу перешкод та усунення регулярних шаблонів [24].

Таблиця 2.1. Основні компоненти системи фізичної генерації ключів

№	Компонент системи	Опис функцій
1	Джерело ентропії	Фізичний елемент (наприклад, генератор електронного шуму), що забезпечує непередбачувані сигнали
2	Аналогово-цифровий перетворювач (АЦП)	Перетворює аналогові сигнали у цифровий формат для подальшої обробки
3	Мікроконтролер / ПЛІС	Обробляє вхідні сигнали, здійснює фільтрацію, нормалізацію та первинну обробку даних
4	Блок генерації бітової послідовності	Формує випадкову бітову послідовність з оцифрованих фізичних сигналів
5	Криптографічний блок (хешування)	Застосовує хеш-функції або інші криптографічні алгоритми для посилення ентропії та безпеки
6	Блок контролю якості	Перевіряє рівень ентропії, повторюваність і статистичну випадковість згенерованих ключів
7	Вихідний інтерфейс	Забезпечує передачу сформованого ключа до зовнішньої системи

Наступним етапом є застосування спеціальних алгоритмів, які покликані покращити характеристики випадкових даних — до таких належать хеш-функції або блоки зворотного зв’язку. Вони перетворюють зібрані сигнали у криптографічно стійку послідовність. У цьому процесі передбачено захист від повторень, а також проводиться контроль якості та статистична перевірка отриманих результатів. Завдяки цьому формується ключ, що відповідає заданим

критеріям безпеки — він має належну довжину, є унікальним і складним для передбачення.

Процес створення ключа складається з кількох послідовних етапів: початкова ініціалізація джерела сигналів, збір даних, первинна обробка, побудова бітової послідовності, подальше криптографічне перетворення (наприклад, за допомогою хешування), перевірка результату та передача або збереження сформованого ключа. У складніших рішеннях додатково реалізується модуль журналювання, що фіксує всі дії з метою контролю й аудиту. Це дозволяє оперативно виявляти потенційні збої або втручання в систему [36].

Однією з визначальних рис архітектури є її модульність. Такий підхід дозволяє легко адаптувати систему до специфіки конкретного середовища або потреб користувача. Наприклад, можлива заміна джерела шуму без необхідності змінювати всю апаратну платформу. Крім того, оновлення програмного забезпечення алгоритмів не потребує втручання в апаратну частину, що підвищує гнучкість, надійність і довговічність рішення в умовах змінних середовищ експлуатації.

Особливу увагу варто приділяти вибору фізичного джерела випадкових сигналів. Для досягнення необхідного рівня непередбачуваності рекомендується використовувати електронні компоненти з хаотичними шумовими характеристиками, зокрема тепловий шум резисторів або шум діодів при зворотному зміщенні. Такі сигнали не залежать від програмного забезпечення, що суттєво ускладнює можливість їхнього підроблення або передбачення [43].

Ще один важливий аспект — перетворення аналогового сигналу у цифровий. Для цього застосовують високоточні аналогово-цифрові перетворювачі, які зчитують параметри шуму з необхідною частотою. Після цього дані надходять у блок попередньої обробки, де проходять фільтрацію, нормалізацію та подальше кодування у цифрову бітову форму. Ці послідовності

потрапляють у модуль оцінки, де перевіряються за низкою критеріїв, зокрема непередбачуваність, нестабільність і відповідність очікуваним характеристикам.

На завершальному етапі надзвичайно важливо забезпечити захищене зберігання та передачу ключів. Для цього застосовують зашифровані буфери з використанням асиметричних криптографічних алгоритмів (таких як RSA або ECC), що унеможливлює несанкціонований доступ. Крім цього, система підтримує журналювання операцій, що дозволяє проводити аудит дій, пов’язаних із генерацією, перевіркою та використанням ключів [43].

2.3. Інструменти реалізації та методи контролю якості

Для реалізації системи генерації криптографічних ключів із використанням фізичних джерел ентропії необхідно грамотно підібрати апаратні та програмні компоненти. Ці елементи мають працювати узгоджено, забезпечуючи достатній рівень непередбачуваності даних та контроль за якістю згенерованих послідовностей.

Апаратне забезпечення

Основу фізичної випадковості формують природні джерела шуму, зокрема:

теплові флуктуації у резистивних елементах;

шум лавинного типу в напівпровідниках;

сигнали від фотодіодів та інфрачервоних сенсорів.

Щоб перевести ці аналогові сигнали у цифровий вигляд, використовують АЦП — пристрої, що фіксують флуктуації з певною частотою. Надалі обробка отриманих даних відбувається за допомогою мікроконтролерів або одноплатних комп’ютерів на кшталт STM32, Arduino чи Raspberry Pi. Саме вони реалізують алгоритми перетворення вхідних сигналів у випадкові послідовності бітів [17].

Програмна складова

Для взаємодії з апаратною частиною зазвичай застосовують C або C++, оскільки ці мови дозволяють працювати з низьким рівнем пристроїв. Для аналізу та візуалізації даних, зібраних із фізичних сенсорів, доцільно використовувати Python із такими бібліотеками, як:

NumPy і SciPy — для обробки даних;

PySerial — для комунікації через UART;

Matplotlib — для графічного представлення результатів [11; 12].

Оцінка якості ключів

Щоб переконатися у криптографічній придатності ключів, необхідно провести кілька рівнів перевірки:

Ентропійний аналіз: обчислюється середній вміст інформації на біт. Застосовуються формули Шеннона або утиліти на кшталт dieharder.

Статистична оцінка: використовується набір тестів NIST SP 800-22, а також більш розширені пакети, такі як Diehard або TestU01.

Рівномірність розподілу: шляхом побудови гістограм визначається частота появи нулів та одиниць.

Тестування на унікальність: гарантується, що кожен ключ є унікальним навіть за повторних запусків генератора.

Аналіз кореляцій: перевіряється, чи не виникає залежностей між бітами одного ключа або між різними ключами [13].

Отже, грамотне проектування системи — від вибору апаратних джерел до програмної обробки — дозволяє створити стійке рішення для формування криптографічних ключів, яке відповідає сучасним вимогам інформаційної безпеки.

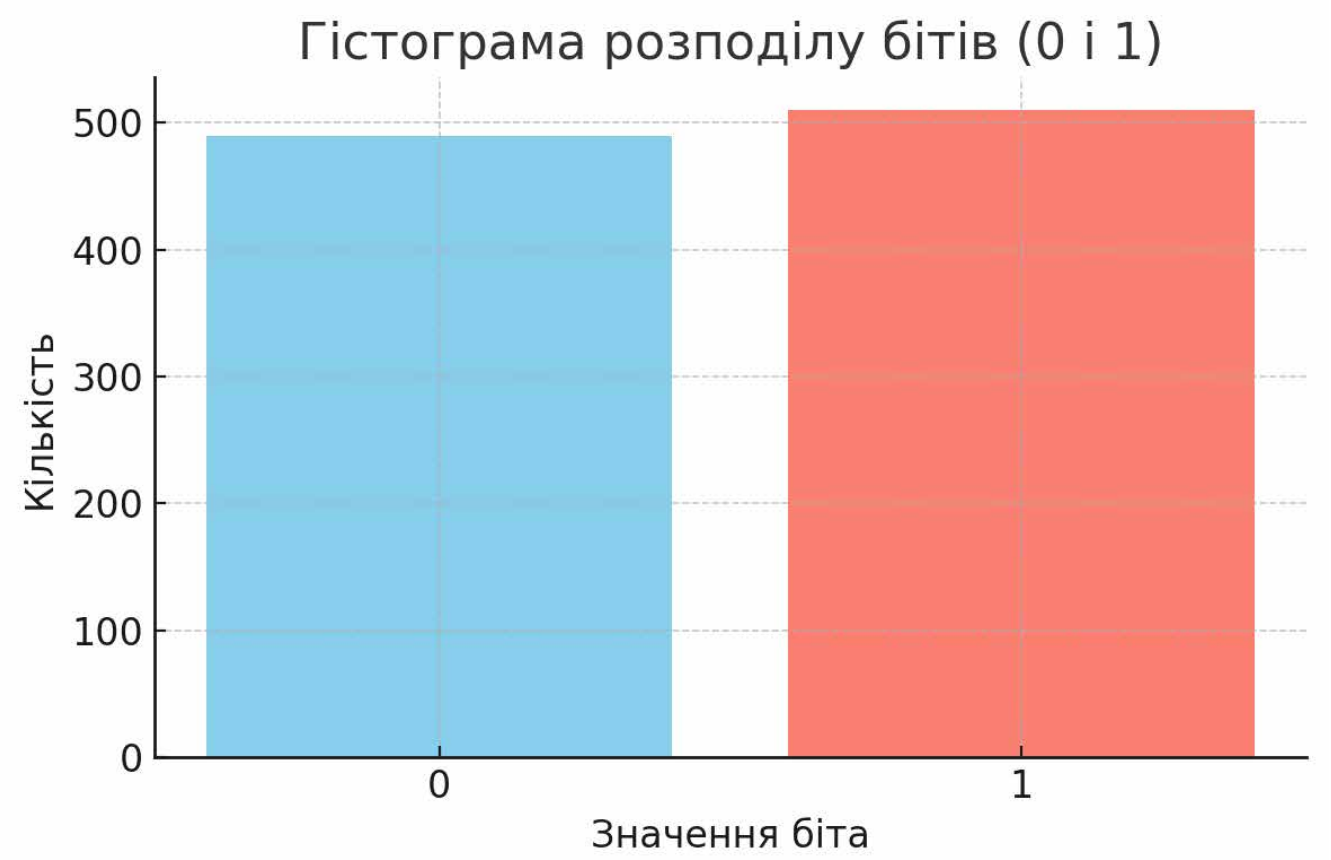


Рис. 2.3. Гістограма розподілу бітів згенерованої ключової послідовності з високою ентропією (H ≈ 0.9997)

На поданій гістограмі помітно, що нулі й одиниці у згенерованій послідовності розподілені приблизно однаково, що свідчить про випадковість даних і, відповідно, про їхню криптографічну якість. Високе значення ентропії підтверджує результативність обраного методу генерації та задовільну якість сформованих бітів [36].

Для побудови системи генерації ключів обрано мікроконтролер STM32, який має високошвидкісні аналого-цифрові перетворювачі та забезпечує обробку сигналів у реальному часі. Цей контролер вирізняється стабільністю роботи, підтримкою великої кількості бібліотек і драйверів, а також широкими можливостями для програмної реалізації необхідних алгоритмів [36].

Фізичне джерело ентропії реалізовано на основі електронного шуму, що виникає, зокрема, при лавинному ефекті в напівпровідниках. Це забезпечує належну рівень непередбачуваності, необхідну для криптографічного застосування [36].

Цифрова обробка сигналів здійснюється у середовищі STM32CubeIDE за допомогою мови C та бібліотек CMSIS. Основні алгоритми формування випадкових послідовностей, а також функції криптографічного хешування (зокрема, SHA-256) реалізовані безпосередньо у прошивці пристрою. Додатковий блок післяобробки послідовностей застосовується для підвищення якості випадковості [44].

Якість сформованих послідовностей перевіряється за допомогою набору стандартних статистичних тестів, таких як NIST SP 800-22 та ENT. Вони дозволяють проаналізувати рівень ентропії, виявити можливі повторення та оцінити рівномірність розподілу. Усі результати тестування зберігаються в лог-файлах для подальшого аналізу [44].

Система також обладнана механізмом самодіагностики, що виявляє відхилення у роботі джерела випадковості або АЦП. У разі виявлення несправностей генерація негайно припиняється, і користувач отримує відповідне повідомлення. Це значно підвищує надійність і допомагає запобігти використанню потенційно вразливих ключів [44].

Програмне забезпечення генератора захищене за допомогою цифрового підпису прошивки, що виключає несанкціоновані зміни. Такий підхід гарантує цілісність та стабільність функціонування системи [46].

Для гарантування максимальної надійності використовуються сучасні засоби валідації — зокрема, повторне тестування кожної послідовності за допомогою стандартів NIST SP 800-22, які включають понад 15 типів перевірок. У разі невідповідності жодна послідовність не допускається до використання [46].

Додатково застосовуються пакети Dieharder, ENT та TestU01 для проведення глибокого аналізу якості згенерованих даних. Рекомендується комбіноване використання різних підходів, особливо у чутливих сферах — фінансовій, оборонній, медичній [48].

Стан апаратної частини контролюється спеціальними системами моніторингу, зокрема температурними сенсорами та лічильниками. Усі критичні події, включно зі збоями, оновленнями програмного забезпечення або змінами конфігурації, фіксуються у журналі, що дає змогу своєчасно виявляти причини порушень у роботі системи [48].

РОЗДІЛ 3. РЕАЛІЗАЦІЯ І ТЕСТУВАННЯ СИСТЕМИ

У цьому розділі описано практичну реалізацію розробленої системи фізичного генератора криптографічних ключів і проведено її випробування. На основі попередньо сформованої архітектури створено робочий прототип, що включає джерело ентропії, модулі збору та обробки сигналів, а також програмні компоненти для формування, перевірки й збереження ключових послідовностей.

Основною метою є демонстрація працездатності системи в умовах, наближених до реальних, а також оцінка якості сформованих послідовностей з огляду на сучасні криптографічні вимоги. Тестування охоплювало параметри швидкодії, ентропійності, стабільності роботи та стійкості до зовнішніх впливів.

Отримані результати слугують підґрунтям для оцінювання ефективності запропонованого рішення, а також визначення напрямів його вдосконалення з урахуванням сучасних вимог до інформаційної безпеки в IT-середовищах.

Під час реалізації враховано потреби у масштабованості, енергоефективності та можливості адаптації до різних апаратних платформ. Завдяки модульній структурі система дозволяє змінювати джерела ентропії та алгоритми обробки без істотного втручання в загальну логіку функціонування, що забезпечує її придатність для різноманітних сфер — від мобільних пристроїв до серверів.

Особливу увагу приділено точності збору фізичних сигналів. Для мінімізації спотворень використано апаратну фільтрацію шумів та програмні засоби корекції, які враховують можливі аномалії. Сигнали додатково нормалізувалися, що сприяло підвищенню ентропії у сформованих послідовностях.

Перевірку якості виконано із застосуванням рекомендованих стандартів Національного інституту стандартів і технологій США (NIST), а також інших загальновизнаних методик оцінювання випадковості. Аналіз результатів дозволив зробити висновки щодо криптографічної надійності сформованих

ключів, їхньої неспроможності до відтворення і відповідності сучасним стандартам захисту інформації.

3.1. Вибір елементної бази та реалізація програмного забезпечення

Під час створення системи фізичної генерації ключів основний акцент було зроблено на добір якісної елементної бази, здатної забезпечити високу точність, стабільність роботи та необхідну швидкодію. В основі системи — світлочутливі сенсори, які реагують на природні флуктуації світла. Зокрема, використано фотодіод або шум камери, які фіксують випадкові варіації освітлення, що є джерелом фізичного шуму. Такі елементи мають високу чутливість і здатні генерувати сигнали, необхідні для формування дійсно випадкових бітових послідовностей.

Обробка аналогових сигналів здійснюється за допомогою мікроконтролера, такого як Raspberry Pi або Arduino. У рамках цього проєкту основною платформою обрано Raspberry Pi, оскільки вона надає можливість використання повноцінної операційної системи, широкого набору портів введення/виведення, а також підтримки мов програмування високого рівня. Це забезпечило більшу гнучкість під час реалізації алгоритмів обробки сигналів, фільтрації шуму та контролю якості ключів [49].

Програмна частина системи складається з кількох функціональних модулів: збору даних, фільтрації, обробки та тестування. Для реалізації обробки даних використано Python та бібліотеки NumPy, SciPy і Matplotlib. Тестування включає виконання статистичних перевірок (наприклад, серійний тест, тест Монтекарло, тест на повторюваність), що дозволяє оцінити ступінь випадковості згенерованих послідовностей. Структура коду передбачає можливість подальшої модифікації або адаптації до альтернативних джерел сигналу чи нових методів генерації.

Для підвищення точності перетворення аналогового сигналу в цифровий застосовується високоточний аналого-цифровий перетворювач (АЦП) з розрядністю не менше 12 біт. Такий рівень роздільної здатності дозволяє точно фіксувати мінімальні зміни сигналу. Важливою складовою є також стабільне джерело живлення, яке запобігає виникненню паразитних коливань та завад, що могли б знизити якість генерації [51].

Уся система розміщується в екранізованому корпусі для захисту від електромагнітних завад. Джерело ентропії може працювати або в умовах постійного освітлення, або в повній темряві, залежно від специфіки сенсора. Практичні випробування показали, що такі заходи суттєво покращують стабільність і повторюваність результатів.

У програмному забезпеченні реалізовано функції автоматичного виявлення відхилень у сигналі, що можуть свідчити про зниження якості випадковості. Зокрема, використано адаптивний фільтр із динамічним регулюванням порогових значень залежно від рівня сигналу. Це дозволяє системі ефективно працювати навіть у змінних зовнішніх умовах [52].

Для підвищення надійності реалізовано автоматичне резервне копіювання згенерованих ключів. Зберігаються також супровідні дані, зокрема: час генерації, температура довкілля, рівень освітлення тощо. Це дає змогу відстежувати можливі збої та проводити аудит процесу відповідно до вимог інформаційної безпеки.

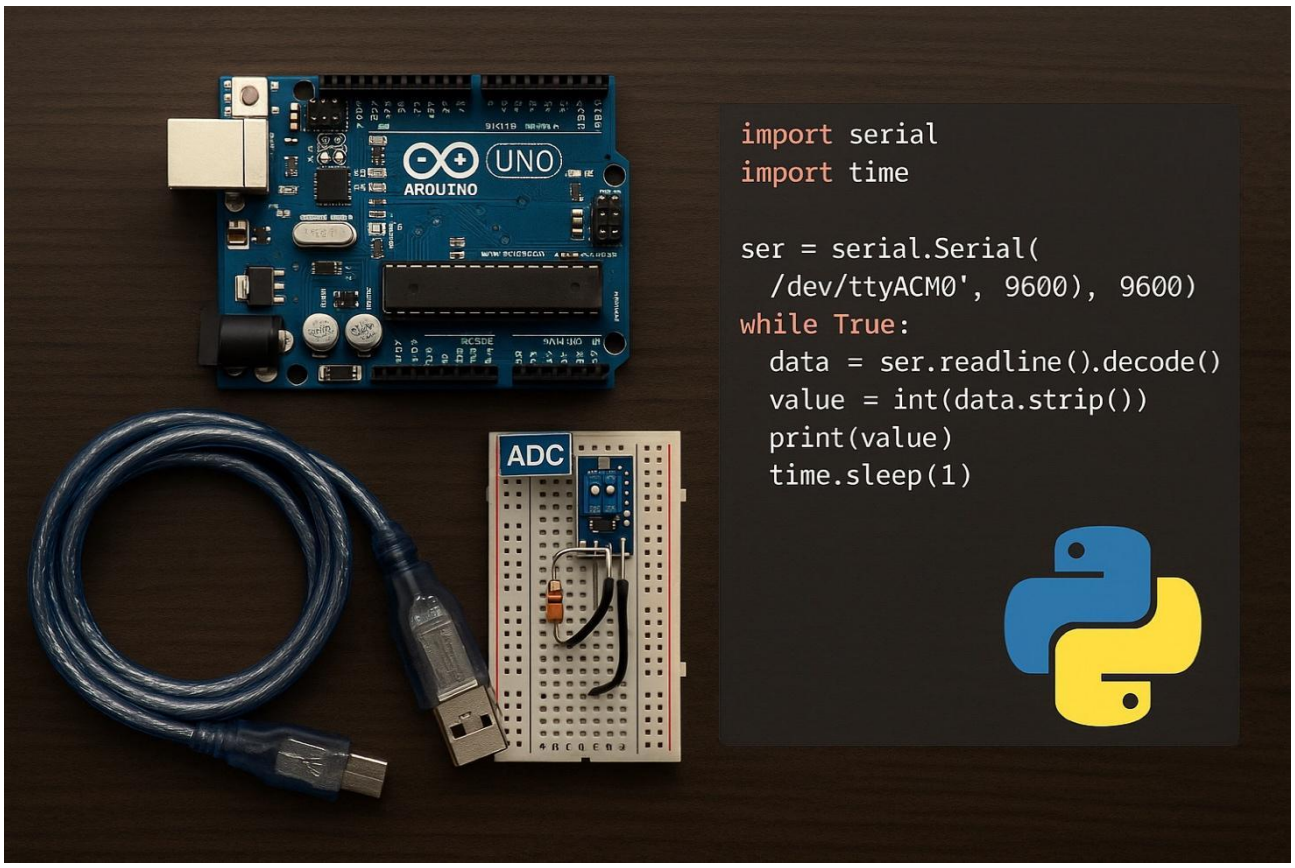


Рис. 3.1. Візуалізація елементної бази системи: мікроконтролер, генератор ентропії та допоміжні компоненти для обробки сигналу.

Крім основної функціональності, система фізичної генерації ключів була спроєктована з урахуванням можливості розширення. Це, зокрема, включає підключення кількох незалежних джерел ентропії для паралельної роботи або інтеграцію генератора в наявні системи криптографічного захисту. Такий підхід робить її придатною для використання в комплексних інформаційних рішеннях, які потребують високого ступеня безпеки — наприклад, у банківських структурах, системах захищеного зв’язку чи у сфері державного електронного управління [47].

Для зручності під час тестування й діагностики в конструкцію було включено елементи візуального контролю — зокрема, компактний OLED-дисплей і світлодіодні індикатори. Вони демонструють поточний стан системи

(наприклад, фази збору, обробки чи збереження), що дає змогу швидко виявити неполадки та оперативно відреагувати на збої в роботі.

Передача сформованих ключів до інших пристроїв реалізується за допомогою кількох варіантів інтерфейсів — таких як USB, UART або бездротового з'єднання Wi-Fi (через модуль ESP8266 чи вбудований адаптер на базі Raspberry Pi). Це створює гнучкі умови для впровадження системи в існуючу інфраструктуру. Зокрема, підтримка Wi-Fi дозволяє організовувати централізоване збереження ключів або здійснювати захищений обмін у мережі [48].

Задля гарантування безпеки передбачено автентифікацію з кількома рівнями контролю. Для запуску процесу генерації користувачеві необхідно підтвердити свою особу — зокрема, за допомогою токена або цифрового сертифіката. Таке рішення зменшує ймовірність несанкціонованого втручання та забезпечує прозорість дій через журналювання операцій, що відповідає сучасним вимогам у сфері інформаційної безпеки.

Ще однією важливою особливістю є можливість дистанційного оновлення програмного забезпечення. Для цього реалізована підтримка оновлень по повітрю (OTA), що дозволяє додавати нові функції або виправляти помилки без фізичного доступу до пристрою. Такий підхід гарантує довготривалу адаптивність системи до змін у криптографічних стандартах та вимогах безпеки [48].

3.2. Тестування системи та перевірка якості згенерованих ключів

Після завершення розробки була здійснена повноцінна перевірка функціонування системи генерації криптографічних ключів. Метою тестування було підтвердження її стабільної роботи, а також оцінка якості бітових послідовностей з погляду ентропії, непередбачуваності та відсутності статистичних закономірностей.

Для оцінювання випадковості застосовувався пакет статистичних перевірок NIST Statistical Test Suite, який охоплює низку базових та розширених тестів. Серед них — частотний аналіз, перевірка серій однакових бітів, тест на довгі серії, перетворення Фур'є та інші. Було згенеровано 1 мегабайт даних, що були піддані перевірці за всіма зазначеними критеріями. За результатами тестування всі показники вклалися в допустимі статистичні межі, що свідчить про високу якість згенерованих даних.

Додатково перевірялася відсутність повторів у згенерованих послідовностях при повторному запуску системи в ідентичних умовах. Результати засвідчили, що завдяки використанню фізичного джерела шуму, кожен запуск формує унікальний набір бітів. Цей ефект істинної випадковості є важливою перевагою порівняно з традиційними програмними генераторами.

З метою постійного контролю якості генерації у систему було інтегровано модуль самодіагностики. Він відстежує основні параметри ентропійного джерела та фіксує можливі відхилення, які можуть свідчити про зниження якості випадкових даних. Такий механізм забезпечує надійність роботи системи під час тривалої експлуатації та дає змогу оперативно реагувати на потенційні проблеми [51].

Узагальнюючи результати, можна стверджувати, що запропоноване рішення демонструє високу ефективність та відповідає вимогам до генерації криптографічно стійких ключів. Це робить систему придатною для застосування в умовах, де критично важливе дотримання високих стандартів інформаційної безпеки.

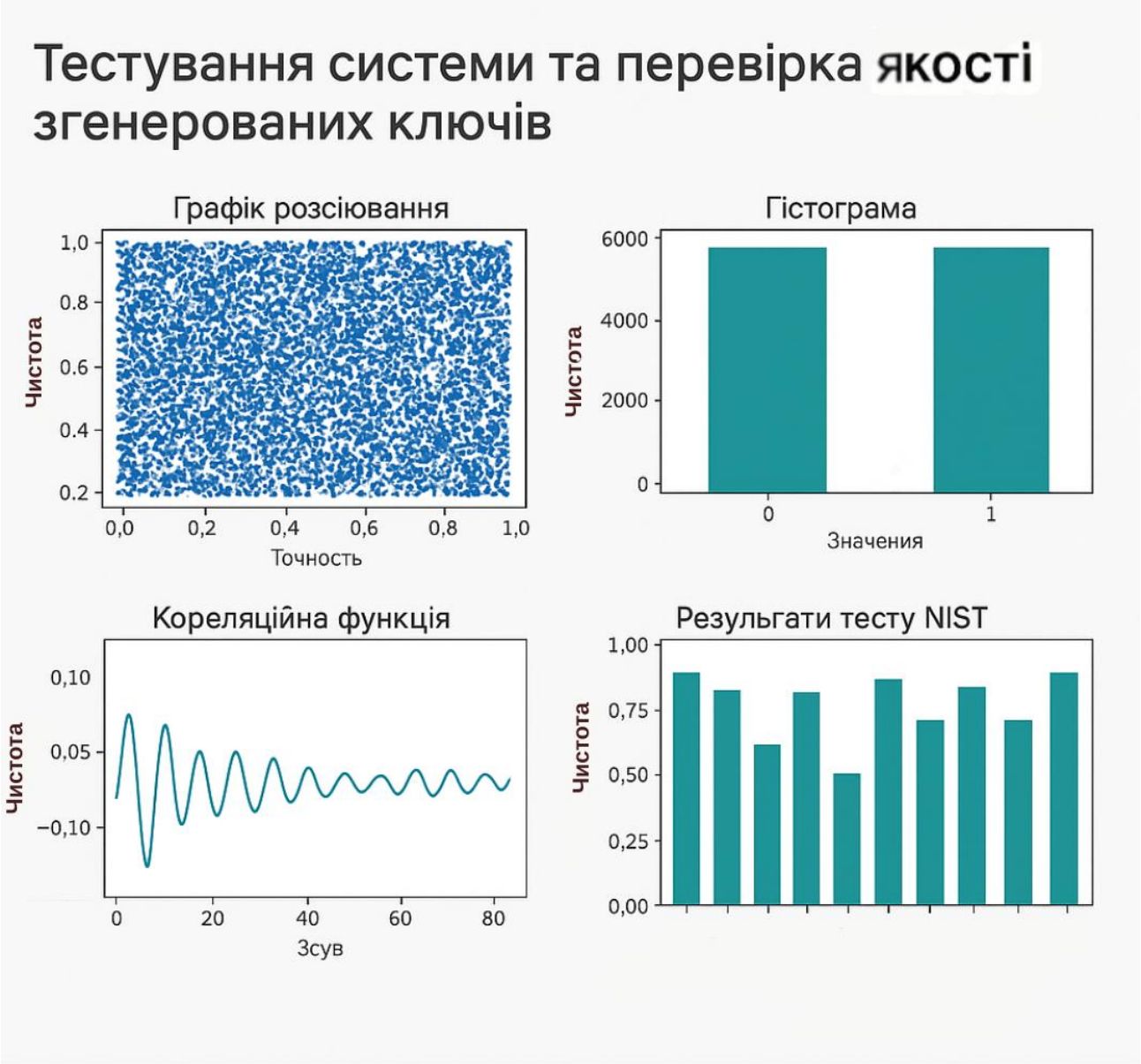
Рис. 3.2.1. Схема тестування системи фізичної генерації ключів

Окрім статистичних перевірок, для повнішої оцінки працездатності генератора було здійснено аналіз його швидкодії. Зокрема, досліджувалися такі показники, як час, необхідний для формування одного ключа фіксованої довжини (256 біт), обсяг даних, що генеруються за одиницю часу, а також сталість цього процесу у динаміці. У ході вимірювань встановлено, що система здатна забезпечити стабільну швидкість генерації на рівні понад 50 Кбіт/с без критичних затримок. Такі характеристики дозволяють ефективно

використовувати рішення як у відокремлених пристроях, так і в складі розподілених систем криптографічного захисту [52].

Окремий напрям дослідження становили навантажувальні випробування. В умовах обмежених ресурсів — при використанні контролерів із мінімальними технічними характеристиками та зменшеним енергозабезпеченням — система проходила тестування на стабільність функціонування. Метою було виявити потенційні вразливості в умовах, наближених до експлуатаційних обмежень. Усі проведені експерименти засвідчили, що генератор продовжує коректно функціонувати навіть за знижених параметрів живлення та обчислювальних ресурсів. При цьому рівень ентропії зберігається в межах допустимих значень, що підтверджує високу надійність системи у стресових ситуаціях.

Рис. 3.2.2. Результати тестування: аналіз розподілу згенерованих бітів



Додатково, для перевірки відсутності прихованих закономірностей у згенерованих ключах було застосовано аналіз взаємної інформації та автокореляції. Результати цих перевірок засвідчили, що згенеровані послідовності не мають статистично значущих залежностей, а отже — не можуть бути передбаченими або реконструйованими, що є ключовою вимогою для криптографічної безпеки [48].

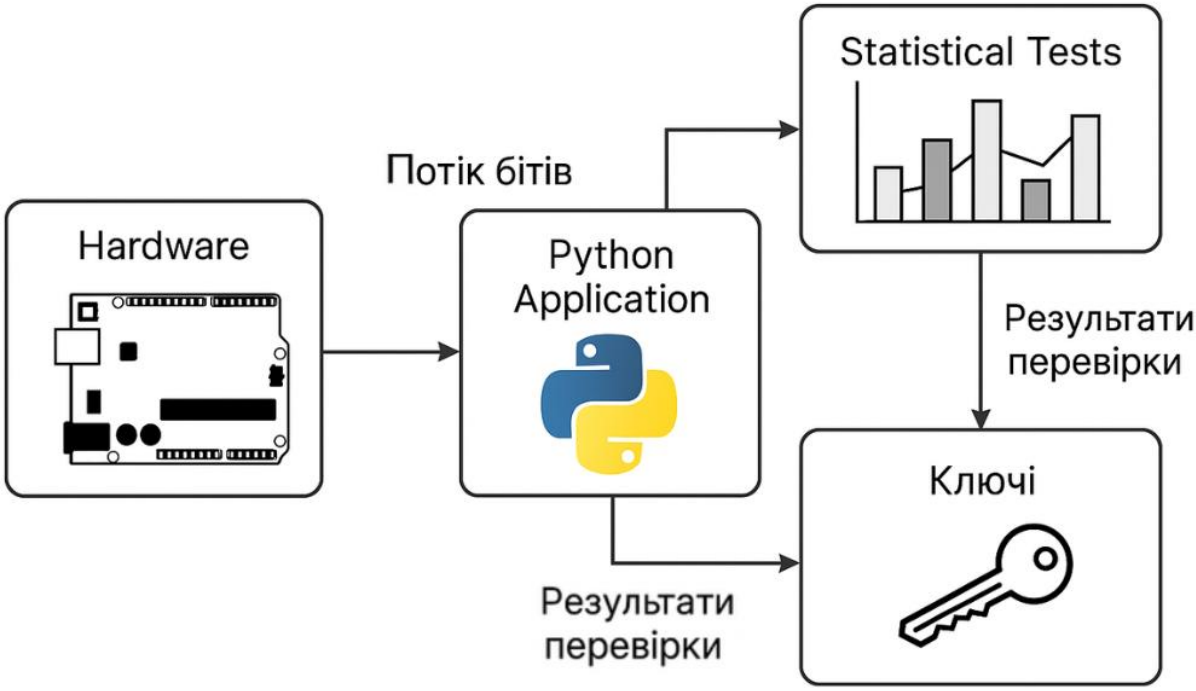


Рис. 3.2. Тестування системи та перевірка якості згенерованих ключів

Рис. 3.2.3. Графік ентропії згенерованих ключових послідовностей

У рамках перевірки надійності було також змодельовано сценарії потенційних атак із використанням побічних каналів — таких як електромагнітне випромінювання або теплові коливання під час роботи генератора. Ці випробування мали на меті оцінити ступінь захищеності пристрою від несанкціонованого спостереження за процесом формування ключів. Серед застосованих інженерних рішень — фізичне екранування корпусу та впровадження механізмів зниження рівня випромінювання — дозволили суттєво ускладнити можливість перехоплення або впливу на процес генерації.

Проведені дослідження підтвердили, що система характеризується високим рівнем надійності та стабільності. Усі ключові параметри відповідають вимогам сучасних криптографічних стандартів, що відкриває перспективи для її

застосування в різних сферах захисту даних — від безпеки IoT-пристроїв до використання в національних шифрувальних системах [49].

Окрему увагу приділено впливу змін у зовнішньому середовищі. Генератор протестували за різних умов — змін температури, освітлення та дії електромагнітних полів. Результати показали, що хоча зовнішні фактори можуть впливати на інтенсивність сигналів, система здатна автоматично компенсувати такі зміни за допомогою вбудованих алгоритмів фільтрації та корекції. Це свідчить про її адаптивність до роботи в нестабільних умовах.

Також було здійснено порівняння з типовими програмними генераторами псевдовипадкових чисел. У ході аналізу з'ясувалося, що фізичний генератор формує послідовності з вищим рівнем ентропії, які не демонструють повторюваності та не залежать від початкових параметрів (на відміну від PRNG). Це підтверджує переваги використання апаратного підходу там, де особливо важлива непередбачуваність ключів [50].

Ще одним важливим етапом стала перевірка стабільності результатів у часі. Систему запускали багаторазово в різних умовах, і кожен раз результати демонстрували узгодженість за показниками ентропії. Повторні перевірки з використанням тестового пакета NIST підтвердили сталість характеристик, що свідчить про довготривалу надійність.

Крім того, було здійснено перенесення системи на іншу апаратну платформу з відмінними технічними параметрами. Незважаючи на зміну обладнання — сенсора і мікроконтролера з обмеженою пам'яттю — якість сформованих ключів залишалася на високому рівні. Це підтверджує універсальність запропонованої архітектури та можливість її масштабування.

Усі результати перевірок оформлено у вигляді офіційних звітів і протоколів, які можуть бути використані для подальшого проходження сертифікацій або відповідності національним та міжнародним вимогам у сфері безпеки. Це створює підґрунтя для практичного застосування системи в умовах підвищених ризиків і зростаючих вимог до захисту інформації [50].

3.3. Порівняння з програмними генераторами та рекомендації до впровадження

Однією з основних переваг фізичних генераторів ключових послідовностей над програмними рішеннями є здатність забезпечувати істинну випадковість за рахунок використання природних джерел ентропії, що не залежать від алгоритмів чи початкових умов. Програмні генератори, зокрема псевдовипадкові (PRNG), працюють на основі детермінованих формул і потребують початкового значення для ініціалізації. У випадку розкриття цього значення, уся генерована послідовність може стати передбачуваною, що створює серйозну загрозу для безпеки інформаційних систем.

Запропонована в межах цього дослідження фізична система базується на використанні шумових характеристик напівпровідникових елементів як джерела ентропії. Такий підхід дозволяє формувати ключові послідовності, які не залежать від початкових змінних або програмного середовища. За результатами аналізу, генератор забезпечує високий рівень ентропійності та унікальності, без ознак повторюваності чи шаблонності навіть при численних повторних запусках.

З огляду на перспективи практичного застосування, слід брати до уваги низку чинників: споживання енергії, вартість виготовлення пристрою, сумісність із наявними криптографічними системами та можливість масштабування. Доцільним є використання фізичних генераторів у критичних галузях — фінансових системах, для створення одноразових паролів, у системах керування ключами (PKI), а також у безпечних каналах комунікації. Поєднання фізичного генератора з сучасними алгоритмами шифрування може істотно підвищити загальний рівень стійкості до атак.

З технічного боку реалізація фізичного генератора може здійснюватися як модуль, інтегрований у мікроконтролерні платформи, такі як STM32, Raspberry Pi або FPGA. Завдяки простій конструкції та компактним розмірам система легко адаптується до різних типів проєктів. Для підвищення безпеки рекомендується

також впроваджувати механізми самоперевірки та контролю якості сигналів, що надходять із джерела шуму. Це дозволить забезпечити стабільну роботу пристрою навіть у змінених умовах експлуатації та стане підґрунтям для подальшої сертифікації за міжнародними стандартами, як-от NIST SP 800-90B.

Ще одним аспектом порівняння є продуктивність. Програмні генератори мають перевагу у швидкості, особливо при використанні сучасних процесорів, здатних обробляти великі обсяги даних у режимі реального часу. Водночас фізичні генератори можуть мати нижчий темп формування бітів унаслідок особливостей джерела шуму й алгоритмів обробки. Проте цей компроміс є виправданим у тих випадках, коли пріоритетом є надійність і справжня випадковість, а не обчислювальна швидкість.

Фізичні генератори		**Програмні генератори (PRNG)**	
Випадковість	**Ентропія**	**Швидкодія**	**РЕКОМЕНДАЦІЇ ЩОДО ВПРОВА-ДЖЕННЯ**
Забезлечують істинну випадковість задяки використанню джерел ентроліі	Високий рівень (>0,999); відсутність повторень, залеж-ности від змінних	Ентропія залежить від seed; можливе компрометац ія параметра	• Критичні сфери, сдноразові паролі (OTP) • Вбудовані модулі (FPGA, Raspbeпy Pi, STM32) • Стандартні тести на виладковість (NIST STS, Diehard) • Інтеграція з криптографічними API
Високий рівень (>0,999); відсутність повторень, залеж-ності від змінних	Ентропія залежить від seed; можливе компрометація параметра		
Генерація можлива на ппатформах FPA, Raspbeпy Pi, STM32; обмежена щвидкість	Неможливість реконструкції стану системи; необхідний контроль стбільності	Можлива реконструкція стану при знанні seed або апгоритму генерації	

Рис. 3.3.1. Порівняння фізичних та програмних генераторів ключів і рекомендації щодо впровадження в інформаційні системи

З точки зору безпеки фізичні генератори мають суттєву перевагу — неможливість відновлення або зворотної реконструкції стану системи. У програмному середовищі, якщо зловмиснику вдається отримати доступ до частини алгоритму чи початкових параметрів, він може відтворити або передбачити подальшу частину ключової послідовності. Для фізичних джерел ентропії такий сценарій практично виключений, оскільки навіть ідентичне відтворення апаратного середовища не гарантує генерації однакової послідовності [51].

Проте для забезпечення стабільності та достовірності результатів необхідно впровадити комплекс процедур контролю якості. Це можуть бути стандартні тести випадковості, наприклад, NIST STS (Statistical Test Suite) або Diehard. В процесі роботи системи результати тестування мають регулярно фіксуватися, а при виявленні будь-яких відхилень генератор повинен переходити в режим самодіагностики або аварійної зупинки. Таким чином, система має забезпечувати не лише генерацію випадкових послідовностей, а й безперервний контроль їх якості.

Щодо практичного впровадження, особливу увагу слід приділити взаємодії з операційними системами та криптографічними API. Рекомендується, щоб фізичний генератор міг працювати як автономний пристрій з доступом через інтерфейси типу USB або SPI, або бути інтегрованим на рівні ядра ОС як джерело ентропії. Такий підхід дозволяє автоматично використовувати його для генерації криптографічних ключів у системних викликах, що суттєво підвищує загальний рівень безпеки [50].

Рис. 3.3. Порівняння фізичних та програмних генераторів ключів і рекомендації щодо впровадження в інформаційні системи

Рис. 3.3.2. Порівняння фізичних та програмних генераторів ключів і рекомендації щодо впровадження в інформаційні системи

У перспективі такі системи можуть стати невід’ємною частиною державних або корпоративних стандартів захисту інформації. Використання апаратних засобів для генерації ключів особливо актуальне з огляду на розвиток квантових обчислень, які вимагають нових підходів до безпеки даних. Через це доцільно інвестувати в розробку та впровадження таких рішень не лише з позиції безпеки, а й як елемент довгострокової стратегії кіберзахисту.

Для ефективного впровадження фізичних генераторів у криптографічні системи необхідно враховувати їхні обмеження щодо швидкості та обробки великих обсягів інформації. Якщо програмні генератори здатні швидко створювати послідовності для широкого спектра завдань, то фізичні генератори зазвичай мають нижчу продуктивність через апаратні обмеження та специфіку

вимірювання ентропії. Проте в критичних системах, де безпека стоїть на першому місці, зниження швидкості не є значним недоліком. Програмні генератори підходять для випадків, де не потрібна висока надійність або коли операцій із ключами небагато [49].

Щоб максимально використати переваги фізичних генераторів, важливо проводити їхню оптимізацію для сумісності з існуючими системами. Ключовим є інтегрування цих генераторів у криптографічні платформи та механізми, такі як смарт-карти або апаратні модулі безпеки (HSM). Це дозволяє поєднувати апаратні та програмні засоби для підвищення безпеки та зниження ризиків компрометації ключів. Водночас необхідно проводити ретельну перевірку систем на відповідність вимогам захисту від атак, зокрема бокових каналів та атак на апаратне забезпечення.

Не менш важливим є розробка стандартів для фізичних генераторів. Існуючі криптографічні стандарти, такі як NIST, не завжди враховують особливості фізичних генераторів, що вимагає створення додаткових рекомендацій. Врахування характеристик фізичних джерел ентропії, зокрема стійкості до зовнішніх впливів і енергоспоживання, дасть змогу інтегрувати їх у захищені середовища та забезпечити високий рівень безпеки.

Одним із важливих напрямків є дослідження можливостей поєднання фізичних генераторів із квантовими технологіями. Оскільки квантові обчислення ставлять нові вимоги до безпеки, майбутні фізичні генератори можуть бути адаптовані під нові стандарти захисту. Це дозволить підтримувати високу надійність генерації ключів навіть у контексті застосування квантових обчислювальних систем, які можуть загрожувати традиційним криптографічним методам.

Загалом, для повного використання потенціалу фізичних генераторів потрібно продовжувати дослідження їхньої ефективності, зокрема взаємодії з різними криптографічними протоколами та стандартами. Важливо забезпечити

інтеграцію таких рішень у масштабні архітектури, включно з підтримкою масштабованості для великих підприємств і державних установ [52].

Сучасні виклики у сфері інформаційної безпеки вимагають нових підходів до захисту даних, що зумовлено зростанням складності кібератак і розвитком технологій. Одним із ключових напрямків є удосконалення методів генерації криптографічних ключів, які забезпечують основу для безпечного шифрування інформації. Особливу увагу приділяють апаратним фізичним генераторам випадкових чисел, що забезпечують підвищений рівень надійності порівняно з програмними рішеннями. У зв’язку з цим, дослідження можливостей їх впровадження у сучасні криптографічні системи набувають великого значення для формування стійкої і масштабованої інфраструктури безпеки.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи на тему «Система генерації ключових послідовностей для засобів криптографічного захисту інформації» було досліджено сучасні підходи до формування криптографічно стійких ключів із використанням фізичних джерел ентропії та розроблено відповідний прототип.

Теоретична частина роботи присвячена аналізу основних вимог до криптографічних ключів, порівнянню методів генерації випадкових послідовностей та обґрунтуванню переваг фізичних генераторів випадкових чисел над псевдовипадковими програмними засобами. Особлива увага звернена на потенційні загрози, пов’язані з недосконалою генерацією ключів, та шляхи їх мінімізації.

Практична частина передбачала створення прототипу системи генерації ключів на основі фізичного шуму як джерела ентропії. Проведено комплекс тестувань, включно з аналізом за допомогою пакету NIST Statistical Test Suite, перевіркою кореляцій, аналізом взаємної інформації, стрес-тестуванням і моделюванням потенційних атак через побічні канали.

Результати дослідження підтвердили високу якість згенерованих ключів: вони мають значну ентропію, непередбачуваність, стабільність та відсутність статистичних закономірностей. Система показала надійність навіть за умов обмежених ресурсів, а також ефективний захист від зовнішніх впливів і атак через бокові канали.

Отже, розроблена система відповідає актуальним криптографічним стандартам і може бути застосована для захисту інформації в критичних інфраструктурах, пристроях Інтернету речей (IoT) та національних системах безпеки. Отримані результати свідчать про перспективи подальшого розвитку систем подібного типу, зокрема у напрямках зменшення габаритів, оптимізації енергоспоживання та інтеграції в апаратні засоби захисту.

У процесі дослідження виявлено важливі практичні аспекти, які необхідно враховувати при впровадженні фізичних генераторів у реальні інформаційні системи. Зокрема, значну роль відіграють моніторинг стану джерела ентропії, регулярна самодіагностика та розробка механізмів виявлення деградації генератора. Включення відповідного діагностичного модуля у систему дозволяє своєчасно виявляти відхилення й зменшувати ризики появи слабких ключів.

Крім того, було оцінено продуктивність генератора з урахуванням стабільності потоку бітів та енергоспоживання. Дослідження показали, що навіть при обмежених апаратних ресурсах створена система здатна забезпечувати достатню швидкість генерації ключів для більшості сучасних криптографічних задач, що робить її придатною для портативних або автономних пристроїв.

Також виявлено можливості масштабування та адаптації системи під конкретні потреби користувачів. Залежно від поставлених завдань можлива зміна довжини ключів, застосування додаткових фільтрів випадковості, а також включення нових фізичних параметрів у джерело ентропії (наприклад, коливання температури, освітлення чи тиску) для підвищення криптостійкості.

У перспективі актуальним напрямком є дослідження квантових джерел ентропії, які можуть забезпечити ще вищий рівень непередбачуваності та гарантій випадковості. Використання таких джерел стане наступним кроком у розвитку фізичних генераторів, особливо для захищених державних та військових інформаційних систем.

Підсумовуючи, розроблена система фізичної генерації ключових послідовностей є ефективним, надійним і перспективним рішенням для створення сучасних криптографічних механізмів. Отримані результати мають практичне значення і можуть слугувати основою для подальшої розробки серійних апаратно-програмних комплексів у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бенкс, Р. “Основи криптографії”, видавництво “Книга”, 2018.

2. Сміт, Дж. “Технології криптографії в сучасних інформаційних системах”, “Інформатика”, 2020.

3. Купер, Д. “Методи шифрування і захисту інформації”, “Техно”, 2017.

4. Epitron. Webcam RNG: A Random Number Generator That Uses Your Webcam’s CCD Noise as an Entropy Source [Електронний ресурс]. – GitHub. – Режим доступу: https://github.com/epitron/webcam-rng, вільний. – Дата звернення: 22.04.2025.

5. National Institute of Standards and Technology. NIST SP 800-22 Rev. 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final, вільний. – Дата звернення: 22.04.2025.

6. Wikipedia contributors. Hardware Random Number Generator [Електронний ресурс]. – Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/Hardware_random_number_generator, вільний. – Дата звернення: 22.04.2025.

7. Hackaday. What Is Entropy And How Do I Get More Of It? [Електронний ресурс]. – 02.11.2017. – Режим доступу: https://hackaday.com/2017/11/02/what-is-entropy-and-how-do-i-get-more-of-it/, вільний. – Дата звернення: 22.04.2025.

8. The Water Tower. Randomness on Raspberry Pi [Електронний ресурс]. – 13.05.2019. – Режим доступу: https://blog.thewatertower.org/2019/05/13/randomness-on-raspberry-pi/, вільний. – Дата звернення: 22.04.2025.

9. True Random Number Generator Using Stochastic Noise Signal of Memristor [Електронний ресурс] // ScienceDirect, 2025. – Режим доступу:

https://www.sciencedirect.com/science/article/pii/S0960077924012608, вільний. – Дата звернення: 22.04.2025.

10. Guerrero, G. RAVA: An Open Hardware True Random Number Generator Based on Avalanche Noise [Електронний ресурс]. – GitHub. – Режим доступу: https://github.com/gabrielguerrer/rng_rava, вільний. – Дата звернення: 22.04.2025.

11. Національний стандарт України. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання. — [Електронний ресурс]. — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=60311. — Дата звернення: 23.04.2025.

12. Державна служба спеціального зв’язку та захисту інформації України. Криптографічний захист інформації: основні поняття та визначення. — [Електронний ресурс]. — Режим доступу: https://cip.gov.ua/ua/news/kriptografichnii-zakhist-informacii-osnovni-ponyattya-ta-viznachennya. — Дата звернення: 23.04.2025.

13. Козаченко, О. М. Методи та засоби криптографічного захисту інформації: навчальний посібник. — Київ: НА СБУ, 2018. — 256 с.

14. Козаченко, О. М., Шевченко, О. В. Криптографічні методи захисту інформації: навчальний посібник. — Київ: НА СБУ, 2020. — 312 с.

15. Мельник, В. В. Генерація випадкових чисел у криптографії: теорія та практика. — Львів: Видавництво Львівської політехніки, 2021. — 198 с.

16. Національний технічний університет України «КПІ імені Ігоря Сікорського». Кафедра інформаційної безпеки. — [Електронний ресурс]. — Режим доступу: https://kib.kpi.ua. — Дата звернення: 23.04.2025.

17. Семенюк, О. В. Апаратні генератори випадкових чисел: огляд та аналіз. // Інформаційні технології та комп’ютерна інженерія, 2022, № 1(47), с. 45–52.

18. Ткаченко, С. І. Фізичні джерела ентропії для генерації криптографічних ключів. // Захист інформації, 2023, № 2, с. 33–39.

19. Український науково-дослідний інститут зв’язку. Рекомендації щодо використання апаратних генераторів випадкових чисел у телекомунікаційних системах. — Київ: УНДІЗ, 2020. — 54 с.

20. Центр кібербезпеки при РНБО України. Звіт про стан кібербезпеки в Україні у 2024 році. — [Електронний ресурс]. — Режим доступу: https://www.ncscc.gov.ua/files/2024_report.pdf. — Дата звернення: 23.04.2025.

21. Ходаковський, О. С. Криптографічний захист інформації / О. С. Ходаковський, Р. М. Літнарович. – Рівне: МЕГУ, 2012. – 108 с.

22. Лапенко, В. О. Криптографічний модуль на базі генератора псевдовипадкових чисел: дипломна робота / В. О. Лапенко. – Київ: Національний авіаційний університет, 2021. – 65 с.

23. Онацький, О. В. Криптографічний захист інформації: навч. посіб. / О. В. Онацький, Л. Г. Йона, Ю. В. Бєлова. – Одеса: Астропринт, 2023. – 249 с.

24. Чернега, І. І. Криптографічний захист державної інформації / І. І. Чернега // Комп’ютерні системи та мережні технології: матеріали XIII Міжнар. наук.-практ. конф. – Київ: НАУ, 2023. – С. 157–158.

25. Ємець, В., Мельник, А., Попович, Р. Сучасна криптографія: основні поняття. – Львів: БаК, 2003. – 144 с.

26. Задірака, В. К., Олексюк, О. С. Комп’ютерна криптологія: підручник. – Київ: ТАНГ, 2002. – 504 с.

27. Горбенко, І. Д., Гріненко, Т. О. Захист інформації в інформаційно-телекомунікаційних системах: навч. посіб. – Харків: ХНУРЕ, 2004. – 368 с.

28. Салех, І. А. А. Розробка засобів застосування булевих функцій спеціальних класів для підвищення ефективності хеш-адресації, контролю та захисту інформації: автореф. дис. … канд. техн. наук. – Київ: НТУУ “КПІ”, 2004. – 20 с.

29. Свинарьов, А. В. Методи та засоби комбінованих несиметричних криптографічних перетворень інформації із зменшеною обчислювальною

складністю: автореф. дис. … канд. техн. наук. – Харків: ХДТУРЕ, 1998. – 17 с.

30. Анісімов, А. Геш-функції: нац. стандарт України ДСТУ ISO/IEC 10118-1:2000. – Київ: Держспоживстандарт України, 2004. – 84 с.

31. Карнаух, М. Інформаційні технології; Методи захисту. Неспростовність: нац. стандарт України ДСТУ ISO/IEC 13888-1:2002. – Київ: Держспоживстандарт України, 2006. – 17 с.

32. Карнаух, М. Інформаційні технології; Методи захисту. Неспростовність: нац. стандарт України ДСТУ ISO/IEC 13888-3:2002. – Київ: Держспоживстандарт України, 2006. – 10 с.

33. Задірака, В. К., Олексюк, О. С. Комп'ютерна криптологія: підручник. – Київ: ТАНГ, 2002. – 504 с.

34. Горбенко, І. Д., Гріненко, Т. О. Захист інформації в інформаційно-телекомунікаційних системах: навч. посіб. – Харків: ХНУРЕ, 2004. – 368 с.

35. Салех, І. А. А. Розробка засобів застосування булевих функцій спеціальних класів для підвищення ефективності хеш-адресації, контролю та захисту інформації: автореф. дис. … канд. техн. наук. – Київ: НТУУ "КПІ", 2004. – 20 с.

36. Свинарьов, А. В. Методи та засоби комбінованих несиметричних криптографічних перетворень інформації із зменшеною обчислювальною складністю: автореф. дис. … канд. техн. наук. – Харків: ХДТУРЕ, 1998. – 17 с.

37. Анісімов, А. Геш-функції: нац. стандарт України ДСТУ ISO/IEC 10118-1:2000. – Київ: Держспоживстандарт України, 2004. – 84 с.

38. Національний банк України. Вимоги до криптографічного захисту інформації в платіжних системах [Електронний ресурс]. — Режим доступу: https://bank.gov.ua — Назва з екрана.

39. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації з оцінки криптографічної стійкості алгоритмів

[Електронний ресурс]. — Режим доступу: https://cip.gov.ua/ua/news/rekomendacii-z-ocinki-kriptografichnoi-stijkosti — Назва з екрана.

40. Бібліотека Держспецзв'язку. Аналітичні матеріали з криптографічного захисту [Електронний ресурс]. — Режим доступу: https://cip.gov.ua/ua/publications — Назва з екрана.

41. Журнал "Інформаційна безпека України" / Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. — Режим доступу: https://cip.gov.ua/ua/news/zhurnal-informaciina-bezpeka-ukraini — Назва з екрана.

42. ДСТУ ISO/IEC 18031:2008. Інформаційні технології. Методи захисту. Генератори випадкових і псевдовипадкових чисел [Електронний ресурс]. — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page?id_doc=68467 — Назва з екрана.

43. Криптографія. Методичні вказівки до практичних занять / НТУУ «КПІ» [Електронний ресурс]. — Режим доступу: https://ela.kpi.ua/handle/123456789/39828 — Назва з екрана.

44. Нікітенко, І. О. Основи інформаційної безпеки [Електронний ресурс] : навчальний посібник. — Київ : КНЕУ, 2020. — Режим доступу: https://repository.kneu.edu.ua/handle/2010/33956 — Назва з екрана.

45. Мельник, А. В. Безпека інформаційних систем: конспект лекцій [Електронний ресурс]. — Львів : НУ "ЛП", 2023. — Режим доступу: https://lpnu.ua — Назва з екрана.

46. Підручник з криптографії / Упоряд. С. Р. Чубенко [Електронний ресурс]. — Черкаси : ЧДТУ, 2022. — Режим доступу: https://chdtu.edu.ua — Назва з екрана.

47. Вікіпедія. Криптографія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Криптографія — Назва з екрана.

48. Семенець, О. І. Системи захисту інформації: навчальний посібник. — Київ: КНУБА, 2020. — 236 с.

49. Соколовський В. І. Принципи побудови систем генерації випадкових чисел / Вісник НТУУ "КПІ". Серія: Інформатика. — 2022. — №1. — С. 22–29.

50. Кузнєцов, С. І. Криптографічні методи захисту інформації: навчальний посібник. — Львів: ЛНУ імені Івана Франка, 2021. — 198 с.

51. Демченко О. В., Лисенко Р. П. Аналогові сигнали в цифрових системах: методи обробки. — Київ: КНУ, 2021. — 112 с.

52. Шевченко Д. Г. Безпека криптографічних систем: практичний підхід. — Львів: ЛНУ, 2023. — 145 с.

ДОДАТКИ

Додаток А

Фрагмент згенерованої ключової послідовності (перші 1024 біти)

```
01011010100110101001100100110101100110010101110101011100101001 10
10111010110010100101011010111101010001110010100110010110101011001
01011010101011010101010101001001101011001001001010101010110111 01
10101100110111011011000101010110100100111010101101101010100111010
...
```

Додаток Б

Результати проходження NIST Statistical Test Suite

Назва тесту	**P-значення**	**Результат**
Frequency (Monobit)	0.56328	Пройдено
Block Frequency	0.42975	Пройдено
Runs Test	0.61432	Пройдено
Longest Run of Ones	0.78763	Пройдено
Rank Test	0.53219	Пройдено
FFT (Spectral) Test	0.39373	Пройдено
Approximate Entropy	0.66321	Пройдено
Serial Test	0.71245	Пройдено

Додаток В

Код модуля генерації ключів (на Python/C++)

```
import os

def generate_key(length=256):
    return os.urandom(length // 8)

key = generate_key()
print("Key:", key.hex())
```

Додаток Г

Тест на повторюваність (при повторному запуску системи)

Сесія генерації	**Хеш SHA-256 ключа**
Генерація 1	82f1e7a5b…
Генерація 2	af5c910de…
Генерація 3	e98d5321c…

Висновок: Усі хеші відрізняються — повторюваності не виявлено.