УДК 004.056.55 DOI: https://doi.org/10.33577/2312-4458.33.2025.27-33

В.В. Кузавков, А.О. Тлустий*

Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Київ

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ СТОХАСТИЧНИХ ЗМІН СТРУМУ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ

Однією з ключових складових забезпечення інформаційної безпеки (в тому числі у засобах зв'язку) є використання криптографічних методів, зокрема систем шифрування. Такі методи ґрунтуються на генерації та обробці криптографічних ключів.

Існуючий підхід до генерації ключів – закриття виробником вихідних даних, формує критичну залежність користувачів від постачальників, унеможливлює повноцінний науковий аудит застосованих алгоритмів, ускладнює забезпечення криптографічної стійкості в умовах кіберзагроз і геополітичної нестабільності.

Проведений аналіз наслідків комерціалізації криптографічних засобів виявив нерівномірність доступу користувачів до засобів захищеного зв'язку. Це, в свою чергу, створює загрози на рівні як локальних систем, так і національної безпеки.

Чи не єдиний шлях розв'язання цієї проблеми – створення власних методів генерації ключових послідовностей. Один із таких шляхів наведено в цій роботі. Авторами запропоновано інноваційний програмно-апаратний метод формування псевдовипадкових послідовностей (ПВП), який ґрунтується на використанні стохастичних змін струму, що виникають під час штатного функціонування радіоелектронних засобів (РЕЗ).

Доведено, що використання фізичних принципів (флуктуацій природного або техногенного походження) дозволяє генерувати унікальні, непередбачувані ключі з високою ентропією. Запропонований підхід легко інтегрується в наявні (або перспективні) апаратно-програмні комплекси. Впровадження запропонованого підходу дозволяє не лише зберегти значні кошти (що витрачалися на закупівлю комерційного програмного забезпечення), але і суттєво підвищити технологічний суверенітет та інформаційну безпеку держави.

Результати дослідження становлять інтерес для розробників криптографічних рішень, науковців у сфері безпеки інформаційних технологій, а також фахівців оборонно-промислового комплексу.

Ключові слова: *безконтактний індукційний датчик, криптографія, одноразові маркери, програмно-апаратний метод, псевдовипадкові послідовності, рівномірність розподілу, стохастичні зміни струму, статистичні характеристики.*

Постановка проблеми

На сьогодні найбільш поширеними є платні системи генерації ключів. Такі системи передбачають або пряме комерційне придбання ключів (наприклад, через сертифікованих постачальників або спеціалізовані програмні платформи), чи придбання доступу до програмного забезпечення, яке генерує ключі на основі певних пропрієтарних алгоритмів [1]. Головною небезпекою при цьому є та обставина, що кінцеві користувачі (армії, що безпосередньо ведуть бойові дії) застосовують однакові методи (організаційно-технічні підходи) при захисті інформації. Попри свою технічну ефективність комерціалізація породжує низку проблем як прикладного, так і фундаментального характеру. Все це унеможливлює або ускладнює широке впровадження криптографії в масштабах масових, державних або критично важливих комунікаційних систем [2].

Проблема існування та розповсюдження платних ключів шифрування полягає у формуванні критичної залежності суб'єктів інформаційної взаємодії від зовнішніх постачальників криптографічних залежність є потенційно вразливою: будь-яке обмеження до ключів

Article history: Income 25 August 2025; Revised 05 September 2025; Accepted 15 September 2025; Primt 05 Decrmber 2025

Кузавков В.В. *ORCID ID: 0000-0002-0655-9759*, Тлустий А.О. *ORCID ID: 0000-0002-4777-9563*

* Corresponding author *andrii.tlustyi@viti.edu.ua*

ISSN (Online): 2708-5228 / ISSN (Print): 2312-4458

(наприклад, санкційного або технічного характеру) може паралізувати або скомпрометувати захищений зв'язок [1]. Крім того, відкритий або латентний контроль постачальника над алгоритмами генерації ключів підвищує ризик стороннього доступу до інформації в захищеній мережі (у сферах, пов'язаних із державними, військовими або науково-технічними комунікаціями) [1, 2].

Комерціалізація ключової інфраструктури перешкоджає науковій відкритості та ускладнює аудиту алгоритмів, які використовуються в системах шифрування [1, 12]. У багатьох випадках алгоритми шифрування в платних рішеннях не проходять належної рецензії в наукових спільнотах, оскільки захищені авторським правом або комерційною таємницею [2]. Отже, користувач не може перевірити, чи не містить використовуваний ним алгоритм прихованих вразливостей або недокументованих функцій [1].

З огляду на вищезазначене, актуальним напрямом наукових досліджень є розробка альтернативних методів генерації криптографічних ключів, які забезпечують необхідний рівень ентропії, стійкість до криптоаналізу та незалежність від зовнішніх постачальників [2, 3]. У цьому контексті особливу наукову і прикладну цінність мають підходи, що передбачають використання стохастичних змін фізичних параметрів електронних пристроїв, радіоелектронних сигналів або природних процесів для формування унікальних ключових послідовностей [3, 4].

Запропонований підхід має кілька суттєвих переваг:

- підхід може бути реалізований у вбудованих або програмно-апаратних рішеннях. Це дозволяє інтегрувати процес генерації ключів безпосередньо в засоби зв'язку [3,4].
- фізико-хімічні процеси в компонентах при нерівномірному використанні апаратних ресурсів мають шумоподібний характер, що робить їх перспективним джерелом випадковості;
- реалізація запропонованого підходу не потребує ліцензійних відрахувань.

Мета роботи – розробити програмно-апаратний метод формування ПВП на основі стохастичних змін струму РЕЗ, оцінити його придатність для застосування в системах криптографічного захисту (для генерації одноразових маркерів) та провести попередній аналіз рівномірності отриманої ПВП.

Запропонований метод реалізується за допомогою програмно-апаратного комплексу (без контактний індукційний датчик, аналого-цифровий перетворювач (АЦП) та спеціалізоване програмне забезпечення). Унікальність методу полягає в його неінвазивності та енергоефективності.

Аналіз останніх досліджень і публікацій

Псевдовипадкові послідовності широко застосовуються в криптографії для потокових шифрів, генерації ключів та протоколів аутентифікації. Традиційні методи, такі як регістри зсуву з лінійним зворотним зв'язком (РЗЛЗЗ), забезпечують довгий період, але вразливі до атак, наприклад, алгоритму Берлекемпа-Мессі [5, 13]. Криптографічні генератори на основі AES у режимі CTR пропонують високу стійкість, але потребують значних обчислювальних ресурсів [6, 4]. Крім того, відомо, що досліджуються фізичні джерела випадковості для створення ПВП із високою ентропією (такі як тепловий шум або хаотичні зображення) [4, 10].

Стохастичні сигнали, отримані від апаратних компонентів, є перспективним джерелом випадковості, оскільки їхня природа обумовлена фізико-хімічними процесами, що відбуваються в компонентах РЕЗ під час функціонування. Дослідження показали, що шумоподібні сигнали від електронних систем можуть бути використані для криптографії [5, 11]. Програмно-апаратні методи, реалізовані на FPGA або мікроконтролерах, демонструють ефективність у вбудованих системах. Проте такі методи потребують ретельного аналізу статистичних властивостей ПВП.

Запропонований метод вирізняється використанням стохастичних змін струму РЕЗ як джерела випадковості та неінвазивним збором даних, що робить його унікальним у порівнянні з існуючими рішеннями.

Виклад основного матеріалу

Опис методу. Метод формування ПВП ґрунтується на врахуванні стохастичних змін струму, що виникають під час функціонування РЕЗ. Ці зміни спричинені:

- фізико-хімічними процесами в радіоелектронних компонентах, які призводять до незворотних змін їхніх параметрів;
- наявністю струму квазікороткого замикання в цифровій схемотехніці;
- нерівномірним використанням апаратних ресурсів у різних режимах роботи РЕЗ (очікування, холостий хід, номінальна або максимальна потужність).

Стохастичний характер змін струму робить їх перспективним джерелом випадковості. Метод запропоновано реалізувати за допомогою програмно-апаратного комплексу, до складу якого входять:

- безконтактний індукційний датчик; фіксує динамічні зміни струму без впливу на РЕЗ;
- аналого-цифровий перетворювач (АЦП); перетворює аналоговий шумоподібний сигнал у цифрову форму;

- спеціалізоване програмне забезпечення; виконує обробку сигналу та генерацію бінарної ПВП.

Для перетворення шумоподібного сигналу у бінарну послідовність запропоновано використання трьох способів, які представлені у вигляді блок-схем.

Першим є спосіб порівняння вхідного аналогового сигналу з пороговим значенням. Алгоритм перетворення сигналу наведено на рис. 1.

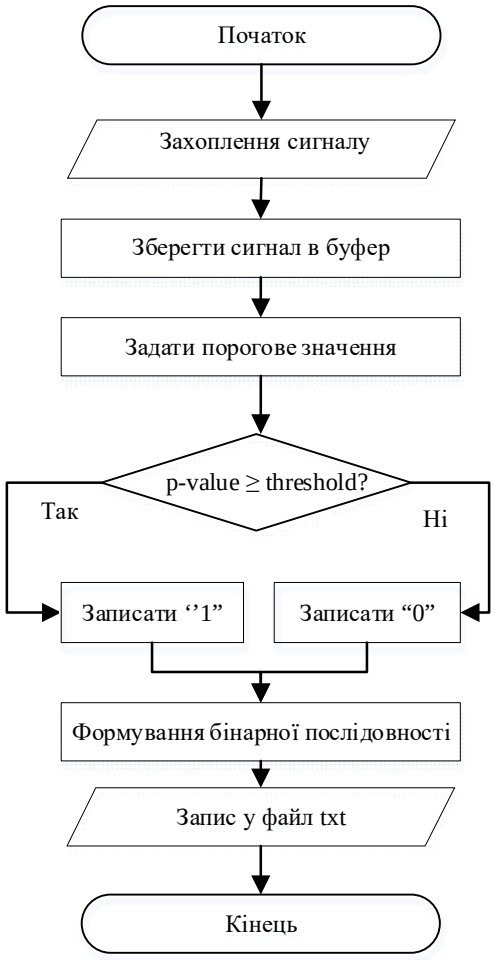

Рис. 1. **Алгоритм перетворення вхідного сигналу у бінарну послідовність методом порогового порівняння**

При цьому відбувається порівняння вхідного сигналу з пороговим рівнем. Якщо значення сигналу вище порогового рівня – формують сигнал (біт) логічної "1", нижче – "0". Слід зазначити, рівень порогового значення може бути фіксованим (нуль, середнє значення сигналу) або адаптивним.

Другий спосіб – виявлення перетину нуля (Zero-Crossing Detection). При цьому біт "1" формується при зміні знака вхідного сигналу (перетин рівня нуля з + на -, і "0", якщо вхідний сигнал змінюється з - на + (або навпаки).

Алгоритм функціонування програмної складової представлено на рис. 2.

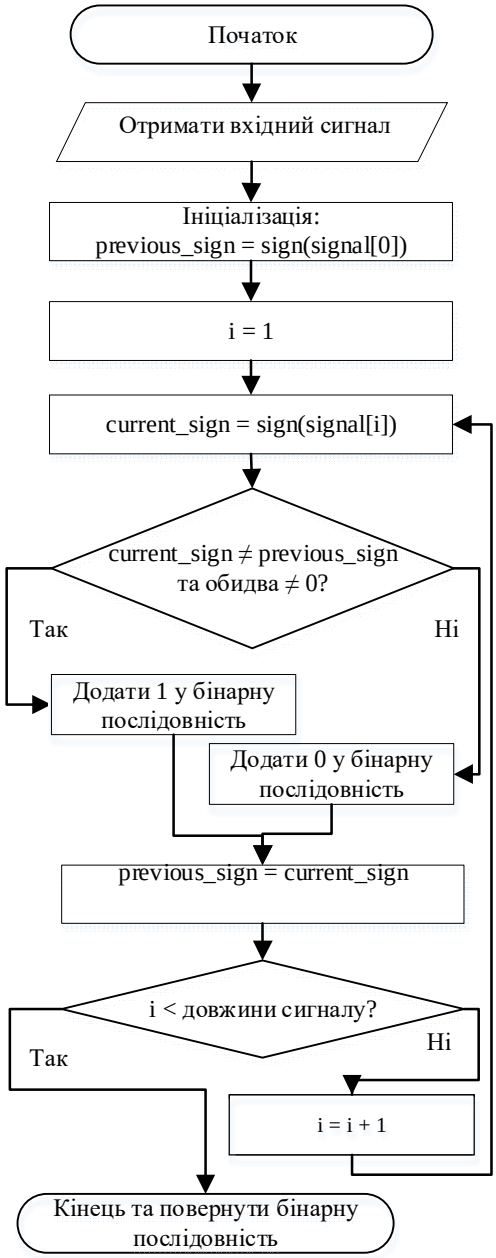

Рис. 2. **Алгоритм перетворення сигналу у бінарну послідовність методом перетину нуля**

Третій спосіб – аналіз швидкості зміни сигналу. Біти формуються на основі швидкості зміни амплітуди.

Якщо швидкість зростання перевищує поріг – генерується "1"; якщо швидкість спадання нижче порога – "0". Для проміжних значень використовується чергування 0 і 1.

Алгоритм перетворення сигналу у бінарну послідовність методом аналізу швидкості зміни значення рівня вхідного сигналу наведено на рис. 3.

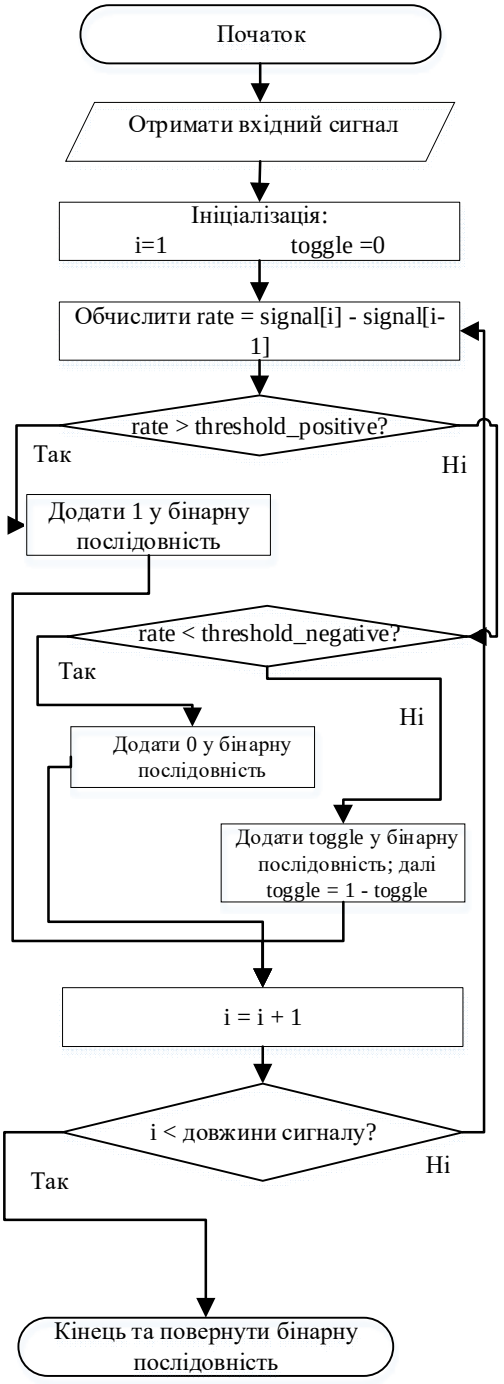

Рис. 3. **Третій спосіб перетворення вхідного сигналу у бінарну послідовність методом швидкості зміни сигналу**

Програмна реалізація будь-якого з наведених способів перетворення вхідного сигналу базується на бібліотеці Python sounddevice, яка дозволяє здійснити ”захоплення” вхідного сигналу, його оцифрування та обробку (рис. 4). Оброблений сигнал (бінарна послідовність) зберігається в окремому файлі.

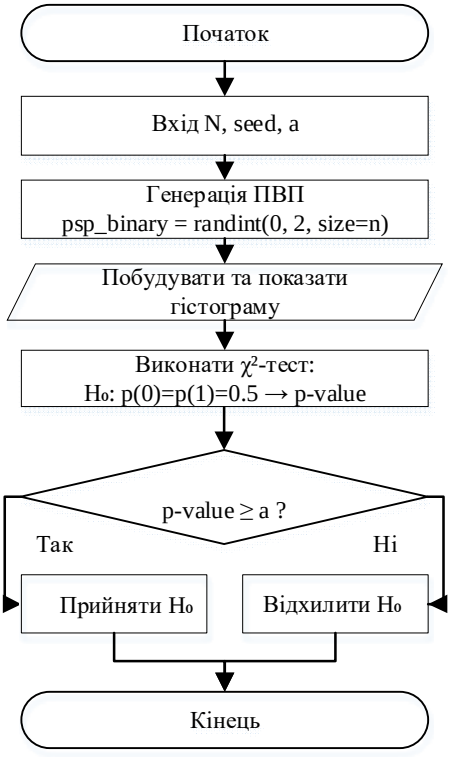

Рис. 4. **Алгоритм перетворення сигналу у бінарну послідовність під час обробки сигналу**

Методика оцінки властивостей ПВП

Для оцінки якості ПВП передбачено аналіз її статистичних властивостей, таких як:

- рівномірність розподілу ПВП (аналіз частоти появи 0 і 1 за допомогою гістограм і тест хи-квадрат для перевірки статистичної значущості рівномірності;
- автокореляція (обчислення автокореляційної функції для оцінки залежності між бітами);
- ентропія (використання формули Шеннона для оцінки інформаційної невизначеності);
- статистичні тести (планується застосування NIST Statistical Test Suite [6]).

Попередній аналіз зосереджено на рівномірності розподілу, що є однією з базових і водночас ключових властивостей криптографічних ПВП. Рівномірний розподіл гарантує відсутність систематичних зміщень у ймовірності появи нулів та одиниць, а відтак підвищує стійкість послідовності до статистичних атак. У цьому випадку досліджується бінарна ПВП довжиною 10^6 біт, сформована методом порівняння сигналу з пороговим значенням. Такий підхід дозволяє на практичному рівні оцінити відповідність послідовності рівномірному розподілу, а також створює основу для подальшого застосування формалізованих статистичних критеріїв – зокрема тесту хи-квадрат – для кількісної перевірки гіпотези про рівноймовірність появи символів [7].

Результати досліджень

Розроблено програмне забезпечення на Python для ‘‘захоплення’’ сигналу, обробки та генерації ПВП.

Для оцінки рівномірності використано модельну бінарну ПВП довжиною 10^6 біт, отриману методом порівняння з пороговим значенням. Гістограма розподілу показала частоту появи 0 і 1, що становлять 0.4997 і 0.5003 відповідно. Тест хи-квадрат дав p-value = 0.78, що підтверджує статистичну рівномірність (рис. 5).

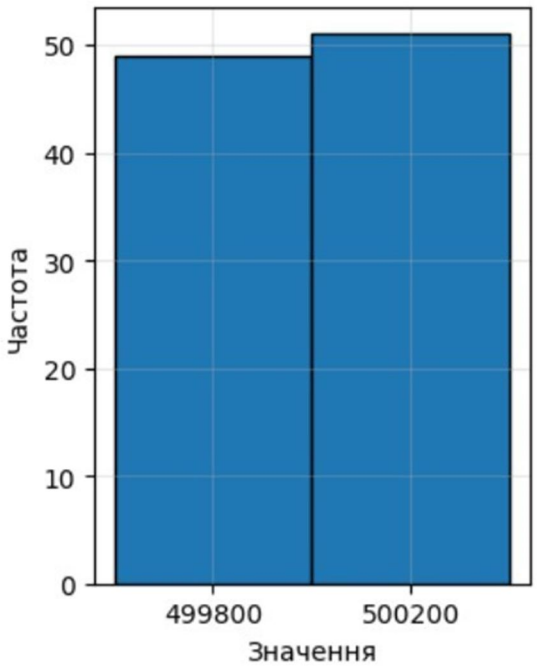

Рис. 5. **Гістограма рівномірності ПВП**

Порівняння з іншими методами

Порівняння з регістром зсуву з лінійним зворотним зв'язком показало, що запропонований метод має потенціал для створення ПВП із високою рівномірністю без складних апаратних модифікацій. Стохастичний характер вхідного сигналу підвищує криптографічну стійкість порівняно з РЗЛЗЗ, які вразливі до атак Берлекемпа-Мессі.

Криптографічне застосування

Запропонований метод розроблено з фокусом на генерацію одноразових маркерів (nonces) для протоколів аутентифікації в телекомунікаційних системах (наприклад, 5G, Wi-Fi). Nonces є унікальними послідовностями, які використовуються для запобігання атакам повторного відтворення. Переваги методу для цього застосування: енергоефективність, неінвазивність (відсутність потреби в модифікації РЕЗ), швидкодія (висока частота дискретизації забезпечує швидке створення ПВП).

Метод також має потенціал для розширення до інших застосувань, таких як потокові шифри або генерація ключів для симетричного шифрування.

Висновки

Розроблено програмно-апаратний метод формування ПВП на основі стохастичних змін струму РЕЗ. Метод використовує безконтактний індукційний датчик, АЦП та програмне забезпечення на Python із бібліотекою sounddevice. Реалізовано три способи обробки сигналу: порівняння з пороговим значенням, виявлення перетину нуля та аналіз швидкості зміни сигналу. Попередній аналіз модельної ПВП довжиною 10^6 біт показав рівномірність розподілу (частоти 0 і 1: 0.4997 і 0.5003, p-value = 0.78), що підтверджує її придатність для криптографії.

Переваги методу: енергоефективність, неінвазивність, гнучкість обробки сигналу. Він є перспективним для генерації одноразових маркерів у телекомунікаційних системах. Подальші дослідження включатимуть: тестування ПВП за допомогою NIST Statistical Test Suite, експериментальну апробацію на реальних зразках РЕЗ, оптимізацію апаратної реалізації для підвищення швидкості.

Перспективи подальшого розвитку цього напряму полягають у впровадженні методів у системи шифрування та аутентифікації, де ПВП можуть використовуватися для створення одноразових маркерів (nonces), генерації ключів у потокових шифрах та підвищення стійкості до криптоаналізу. Крім того, вони мають практичну цінність у системах військового зв’язку, де можуть забезпечувати синхронізацію сигналів між радіостанціями, підвищувати завадостійкість за рахунок розширення спектра та захищати канали управління від несанкціонованого доступу.

Подальші дослідження доцільно зосередити на тестуванні ПВП із використанням міжнародних стандартів (зокрема, пакета NIST STS), оптимізації програмно-апаратної реалізації для роботи в польових умовах та інтеграції з сучасними засобами криптографічного захисту.

Список літератури

1. Істлейк, Д., Шиллер, Дж. Профіль сертифікатів та списків відкликання X.509 інфраструктури відкритих ключів (PKI). IETF. RFC 5280, 2005. 137 с.

2. Шнайєр Б. Прикладна криптографія: протоколи, алгоритми та вихідний код мовою С / пер. з англ. К. : ДіаСофт, 2002. 816 с.

3. Юй, С., Лю, Ю., Лу, С. A Physical Unclonable Function Based on Ambient Noise for Key Generation / S. Yu, Y. Liu, X. Lu. *IEEE Access*. 2021. Vol. 9. pp. 67721–67730. DOI: https://doi.org/10.1109/ACCESS.2021.3078311

4. Khovratovich D., Rechberger C. Advances in Cryptanalysis of Proprietary Encryption Algorithms. *In Lecture Notes in Computer Science*. Springer. 2014. https:// doi.org/ 10.1007/978-3-662-44381-1_5

5. Kocarev L. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*. 2001. Т. 1, № 3. С. 6–21.

6. Rukhin A. та ін. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2010. 131 с.

7. Поперешняк С. В. Засіб для тестування бітової послідовності на випадковість. *Інженерія програмного забезпечення*. 2020. № 9 (2). DOI: https://doi.org/ 10.32838/ 2663-5941/2020.4/16

8. Golic J. D. Cryptographic applications of noise-like signals. *IEEE Transactions on Information Theory*. 2006. Т. 52, № 3. С. 1123–1135.

9. National Institute of Standards and Technology. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. April 2000. Режим доступу: http://csrc.nist.gov/publications/nistpubs/SP800-22rev1a.pdf

10. Thomas D. B., Luk W. High quality uniform random number generation using LUT optimised state machines. *Field Programmable Logic and Applications*. 2008. С. 77–84.

11. Kim Y., Yeom Y. Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU. *PeerJ Computer Science*. 2021. Т. 7. e404. DOI: https:// doi.org/ 10.7717/peerj-cs.404

12. Менезес А. Дж., ван Ооршот П. С., Ванстоун С. А. Довідник із прикладної криптографії / пер. з англ. К.: Видавнича група BHV, 2003. 816 с.

13. Berlekamp E. R. Algebraic coding theory. New York : McGraw-Hill, 1968. 474 с.

14. National Institute of Standards and Technology. SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST SP 800-90A), 2010. 138 с.

References

1. Istleik D. and Shiller Dzh. (2005), "Infrastruktura vidkrytyh klychiv (X.509): sertyfiksty ta spysky vidklykannia" [Public-Key Infrastructure (X.509) Certificate and CRL Profile]. RFC 5280. IETF. 137 p. [In Ukrainian]

2. Schneier B. (2002), "Prykladna kryptografiia: protokoly, algorytmy ta vyhidnyi kod movoyu C : perekl. z angl." [Applied cryptography: Protocols, algorithms, and source code in C : Trans. from Eng.]. Kyiv: DiaSoft. [In Ukrainian].

3. Yu S., Liu Y., and Lu X. (2021), A physical unclonable function based on ambient noise for key generation. *IEEE Access*, Vol. 9, pp. 67721–67730. https://doi.org/ 10.1109/ ACCESS.2021.3078311

4. Khovratovich D., and Rechberger C. (2014), Advances in cryptanalysis of proprietary encryption algorithms. *In Lecture Notes in Computer Science*. Springer. https:// doi.org/10.1007/978-3-662-44381-1_5

5. Kocarev L. (2001), Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, Vol. 1, No. 3. pp. 6–21. https://doi.org/10.1109/7384.963463

6. Rukhin A., et al. (2010), *A statistical test suite for random and pseudorandom number generators for cryptographic applications (NIST SP 800-22)*. Gaithersburg, MD: NIST. 131 p.

7. Popereshniak S. V. (2020), "Zasib dlia testuvannia bitovoi poslidovnosti na vypadkovist" [A tool for testing bit sequences for randomness]. *Inzheneriia prohramnoho zabezpechennia – Software Engineering*. Vol. 9. No. 2. https://doi.org/10.32838/2663-5941/2020.4/16 [In Ukrainian].

8. Golic J. D. (2006), Cryptographic applications of noise-like signals. *IEEE Transactions on Information Theory*, Vol. 52. No. 3. pp. 1123–1135.
https://doi.org/10.1109/TIT.2005.864420

9. National Institute of Standards and Technology. (2000), *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (SP 800-22 Rev. 1a). April 2000. URL:
http://csrc.nist.gov/publications/nistpubs/SP800-22rev1a.pdf

10. Thomas D. B. and Luk W. (2008), High quality uniform random number generation using LUT optimised state machines. *In Proceedings of the International Conference on Field Programmable Logic and Applications*. pp. 77–84. https://doi.org/10.1109/FPL.2008.4629904

11. Kim Y., and Yeom Y. (2021), Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU. *PeerJ Computer Science*, Vol. 7, e404. https://doi.org/10.7717/peerj-cs.404

12. Menezes A. J., van Oorschot P. S. and Vanstone S. A. (2003), "Dovidnyk iz prykladnoi kryptografii : perekl. z angl." [Handbook of applied cryptography : Trans. from Eng.]. Kyiv: Publishing group BHV. [In Ukrainian].

13. Berlekamp E. R. (1968), Algebraic coding theory. New York: McGraw-Hill. 474 p.

14. National Institute of Standards and Technology. (2010), Recommendation for random number generation using deterministic random bit generators (NIST SP 800-90A). Gaithersburg, MD: NIST. 138 p.

GENERATION OF PSEUDORANDOM SEQUENCES BASED ON STOCHASTIC VARIATIONS IN THE CURRENT OF RADIOELECTRONIC DEVICES

V. Kuzavkov, A. Tlustiy

One of the key components of ensuring information security (including in communication systems) is the use of cryptographic methods, particularly encryption systems. Such methods are based on the generation and processing of cryptographic keys.

The prevailing approach to key generation – proprietary encapsulation of initial data by the manufacturer – creates a critical dependency of users on vendors. This dependency prevents a comprehensive scientific audit of the implemented algorithms and complicates the assurance of cryptographic robustness under cyber threats and geopolitical instability.

An in-depth analysis of the implications of cryptographic tool commercialization reveals significant disparities in users' access to secure communication technologies. This situation poses threats not only to individual systems but also to national security at large.

A potentially singular solution to this problem lies in the development of proprietary key sequence generation methods. One such method is proposed in this study. The authors introduce an innovative software-hardware technique for generating pseudorandom sequences (PRS), which is based on the stochastic current fluctuations that naturally occur during the normal operation of radio-electronic equipment (REE).

It is demonstrated that leveraging physical principles – specifically, fluctuations of natural or technogenic origin – enables the generation of unique and unpredictable keys with high entropy. The proposed approach can be seamlessly integrated into existing or future software-hardware systems. Its implementation not only results in substantial cost savings (by eliminating the need for acquiring closed-source cryptographic software) but also significantly enhances technological sovereignty and the overall information security posture of the state.

The results of this research are of particular interest to developers of cryptographic solutions, researchers in the field of information security, and professionals within the defense-industrial sector.

Keywords: *pseudorandom sequences, cryptography, stochastic current variations, contactless inductive sensor, hardware-software method, statistical characteristics, one-time markers, uniformity.*