10. National Institute of Standards and Technology.NIST IR 8545: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf.

11. Dariusz Rzońca, Andrzej Stec, Bartosz Trybus Secure web access to mini distributed control system: Niewielkie rozproszone systemy sterowania ze zdalnym dostępem przez sieć January 2012, Automatyka/Automatics, 16(2) p. 155-164].

12. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 – Proceedings. 2021. P. 67–70.

13. Serhii Yevseiev & Yuliia Khokhlachova & Serhii Ostapov & Oleksandr Laptiev et al, 2023. "Models of socio-cyber-physical systems security," Monographs, PC TECHNOLOGY CENTER, number 978-617-7319-72-5.redif, December. DOI: https://doi.org/10.15587/978-617-7319-72-5.

14. Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Pavlo Open'ko, Volodimir Khoroshko, Lubomir Parkhuts. The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). 2021.Vol 13, No 2, August P.271-277. . DOI : https://doi.org/10.54039/ijcnis.v13i2.5008.

15. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022 P. 93–101. DOI: https://doi.org/10.15587/1729-4061.2022.253530.

16. Oleksandr Laptiev, Andrii Musienko, Volodymyr Nakonechnyi, Andrii Sobchuk, Sergii Gakhov, Serhii Kopytko. Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence.5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 08-10 June 2023

17. DOI: https://doi.org/10.1109/HORA58378.2023.10156702.

Надійшла 21.11.2025

УДК 004.056.55
DOI: 10.31673/2409-7292.2025.041218

Цебак О.А., Войтусік С.С.

МЕТОДИ ОЦІНКИ ЯКОСТІ ТА КРИПТОСТІЙКОСТІ ПОСЛІДОВНОСТЕЙ, ЗГЕНЕРОВАНИХ ГЕНЕРАТОРАМИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

У статті проведено комплексний аналіз методів оцінки якості та криптостійкості генераторів псевдовипадкових чисел (ГПВЧ), які є ключовими елементами сучасних криптографічних систем. Розглянуто декілька основних груп підходів, серед яких статистичні, оцінка криптографічної стійкості, тощо. Статистичні методи, реалізовані у стандартах NIST, дозволяють визначити рівень випадковості послідовностей за такими критеріями, як рівномірність, відсутність кореляцій та ентропічна достатність. Натомість криптографічні підходи зосереджені на перевірці непередбачуваності та стійкості генератора до відновлення внутрішнього стану. Особливу увагу приділено ентропічному аналізу відповідно до вимог NIST SP 800-90B та впливу потенційних квантових атак, що зумовлюють необхідність перегляду існуючих моделей безпеки. Визначено, що жоден окремий метод не забезпечує повної оцінки надійності ГПВЧ, тому найбільш ефективним є комбінований підхід, який поєднує статистичні, криптоаналітичні та ентропічні методи. Запропоновано напрями подальшого розвитку оцінювальних методик, зокрема застосування алгоритмів машинного навчання для виявлення прихованих закономірностей, використання формальних математичних доказів безпеки та створення гібридних систем перевірки, здатних враховувати ризики постквантової криптографії. Отримані результати можуть бути використані для вдосконалення стандартів тестування генераторів та підвищення надійності криптографічних засобів захисту інформації.

Ключові слова: квантові обчислення, криптостійкість, генератори псевдовипадкових чисел, стандарти безпеки, криптографічні системи.

Вступ

Генератори псевдовипадкових чисел (ГПВЧ) є фундаментальним елементом сучасних криптографічних систем, оскільки від їхньої надійності та якості залежить стійкість шифрування, електронних підписів, протоколів автентифікації та інших механізмів захисту інформації. На відміну від звичайних застосунків, де достатньо забезпечити статистичну подібність послідовності до випадкової, у криптографії ключову роль відіграє саме

криптостійкість – здатність ГПВЧ генерувати непередбачувані та стійкі до атак послідовності [17].

Якість випадкових послідовностей визначається двома взаємодоповнюючими аспектами. По-перше, це статистична випадковість, яка передбачає рівномірний розподіл, відсутність кореляцій та закономірностей. По-друге, це криптографічна надійність, що вимагає стійкості до криптоаналітичних методів, неможливості відновлення внутрішнього стану генератора та прогнозування наступних значень навіть за умови знання значної частини вихідної послідовності.

Розробка та вдосконалення методів оцінки ГПВЧ є актуальним завданням у зв'язку з появою нових класів атак, зростанням обчислювальних потужностей, а також у контексті переходу до постквантової криптографії. Традиційні статистичні тести (NIST, Diehard, TestU01) дозволяють виявляти відхилення від випадковості, проте вони не дають повної гарантії криптографічної безпеки. Тому все більшої уваги набувають комбіновані підходи, що поєднують статистичний аналіз із методами криптоаналізу та оцінкою ентропії.

Метою цієї статті є проведення огляду існуючих методів перевірки якості та криптостійкості послідовностей, згенерованих ГПВЧ, а також визначення їхніх переваг, обмежень та перспектив застосування у сучасних криптографічних системах.

Матеріали та методи дослідження

Під час підготовки статті було використано комплексний аналітичний підхід, що поєднує огляд нормативних документів, наукових публікацій і практичних інструментів тестування генераторів псевдовипадкових чисел (ГПВЧ). Основними джерелами інформації слугували міжнародні стандарти NIST SP 800-22, NIST SP 800-90B, класичні пакети тестів Diehard/Dieharder та TestU01, а також праці провідних дослідників у галузі криптографії.

Методологічну основу дослідження становив порівняльний аналіз статистичних і криптографічних методів оцінки якості та стійкості ГПВЧ. Для узагальнення результатів було застосовано елементи системного аналізу, що дозволили виявити взаємозв'язок між статистичною випадковістю, ентропічною складністю та криптографічною надійністю.

Практична частина базувалася на аналізі результатів стандартних тестів, що використовуються у міжнародній практиці для оцінки генераторів випадкових чисел. Зокрема, розглядалися критерії частотності, серійності, ентропії, кореляційних властивостей і структурної складності. Окрім того, у межах теоретичного моделювання враховано аспекти стійкості до відновлення внутрішнього стану генератора, непередбачуваності наступних бітів і впливу квантових атак. Отримані результати були узагальнені з метою формування системного бачення ефективності існуючих методів оцінки та визначення напрямів їх подальшого вдосконалення у контексті постквантової криптографії.

Викладення основного матеріалу

Оцінка послідовностей, згенерованих генераторами псевдовипадкових чисел (ГПВЧ), ґрунтується на поєднанні статистичних і криптографічних підходів. Перші спрямовані на перевірку подібності до істинно випадкових даних, другі — на гарантування неможливості прогнозування або компрометації внутрішнього стану генератора. Сукупне використання цих підходів дозволяє визначити, наскільки конкретний ГПВЧ відповідає вимогам сучасної криптографії. Статистична випадковість означає, що послідовність повинна поводитися подібно до результату «ідеального джерела випадковості». До основних вимог належать:

- Рівномірність розподілу - у великій вибірці частка «0» і «1» повинна бути приблизно однаковою. Якщо частота надмірно відхиляється від 50 %, це свідчить про статистичну аномалію;
- Відсутність кореляцій - наступні біти не повинні залежати від попередніх. Наприклад, якщо після «1» надто часто йде «0», це знижує випадковість;
- Наявність довгих серій та повторів - у випадковій послідовності можливі довгі серії однакових бітів, проте їх частота повинна відповідати ймовірнісним законам;

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

- Складність структури - послідовність не повинна містити простих закономірностей чи циклів, що дають змогу передбачити наступні значення.

Для верифікації цих властивостей застосовують спеціалізовані тестові набори:

- NIST SP 800-22 включає 15 тестів, серед яких тести на частотність, серійність, автокореляцію, лінійність та ентропію. Наприклад, Frequency (Monobit) Test перевіряє баланс «0» і «1», а Approximate Entropy Test – наявність регулярних шаблонів [14].
- Diehard/Dieharder містить класичні перевірки, зокрема Birthday Spacings Test, Overlapping Permutations Test та Rank Test, які виявляють відхилення у довгих послідовностях [11].
- TestU01 є найбільш повним набором (SmallCrush, Crush, BigCrush), який дозволяє протестувати генератори навіть із дуже великою періодичністю [10].

Результати цих тестів часто виражаються через p-значення. Якщо значення занадто близьке до 0 чи 1, це свідчить про те, що послідовність демонструє невипадкові властивості. Водночас успішне проходження статистичних тестів не є гарантією криптографічної безпеки, оскільки навіть повністю «статистично випадковий» генератор може бути вразливим до криптоаналізу.

Криптографічні вимоги значно суворіші за статистичні. Основна мета – забезпечити непередбачуваність послідовності для зловмисника навіть за умови часткового знання чи впливу на систему. До ключових критеріїв належать:

- Непередбачуваність наступного біта. Навіть маючи довгу частину вже згенерованої послідовності, зловмисник не повинен мати змоги передбачити наступний біт із ймовірністю, вищою за 0,5 [12];
- Стійкість до відновлення внутрішнього стану. Наприклад, генератори на базі лінійних регістрів зсуву (LFSR) легко піддаються атакам, якщо отримати достатній обсяг вихідних даних [9];
- Ентропічна достатність. Кількість випадковості (міра Шеннона) має бути достатньою для формування ключів і криптографічних параметрів. У NIST SP 800-90B встановлено вимоги до оцінки ентропії джерел випадковості [15];
- Стійкість до адаптивних атак. Вважається, що атакувальник може підлаштовувати свої дії, маючи частковий доступ до системи. У цьому випадку ГПВЧ повинен залишатися криптографічно безпечним.

Додатково до цих критеріїв сучасні дослідження враховують імовірність квантових атак, які потенційно здатні зменшити складність прогнозування псевдовипадкових послідовностей. Це означає, що класичні ГПВЧ потребують перегляду та вдосконалення для відповідності вимогам постквантової криптографії.

Методи статистичної перевірки

Статистичні методи є базовим інструментом для оцінки якості послідовностей, згенерованих генераторами псевдовипадкових чисел. Їхнє завдання полягає у виявленні відхилень від властивостей істинної випадковості.

Одним із найважливіших тестів у цьому контексті є тест частотності (Frequency Test), який визначає, наскільки кількість нулів і одиниць у довгій послідовності збалансована. Якщо відхилення є надто великим, можна зробити висновок, що генератор має схильність до вироблення певного значення частіше, ніж іншого, що порушує фундаментальний принцип рівномірності [14].

Не менш значущим є тест серій (Runs Test), який перевіряє наявність послідовностей однакових бітів. У випадковій послідовності подібні серії можуть виникати, проте їхня кількість та довжина повинні підкорятися певним ймовірнісним закономірностям. Надто довгі або, навпаки, надто короткі серії свідчать про систематичні закономірності в роботі генератора. Саме цей тест дозволяє відрізнити справді випадкову послідовність від такої, що формально відповідає частотному розподілу, але демонструє приховану регулярність [11].

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

Рис. 1. Методи статистичної оцінки

Ще одним ключовим методом є тест рангу матриць (Rank Test), який застосовується для аналізу випадковості у багатовимірному представленні даних. Послідовність бітів у цьому випадку розглядається як набір матриць, ранги яких повинні відповідати розподілу, властивому для істинно випадкових даних. Якщо спостерігається зниження рангу, це може свідчити про наявність прихованих лінійних залежностей у послідовності, що особливо небезпечно для криптографічних застосунків [10].

Окреме місце займає тест приблизної ентропії (Approximate Entropy Test). Він оцінює різноманітність шаблонів у послідовності, визначаючи, наскільки рівномірно з'являються всі можливі підмножини певної довжини. У випадковому потоці кожен можливий шаблон має з'являтися з приблизно однаковою ймовірністю. Відхилення від цієї закономірності означає, що генератор формує повторювані структури, які можна використати для передбачення наступних значень [14].

Застосування цих тестів у комплексі дає змогу виявляти як найпростіші відхилення, пов'язані з дисбалансом між нулями та одиницями, так і складніші структурні залежності, що формуються на довгих відрізках послідовностей. Саме тому у відомих стандартизованих пакетах, таких як NIST SP 800-22 чи TestU01, вони використовуються як базові та обов'язкові. Однак варто наголосити, що навіть повне проходження цих перевірок не є достатнім критерієм криптографічної стійкості, оскільки вони зосереджені виключно на статистичних властивостях і не враховують потенційних атак, спрямованих на відновлення внутрішнього стану генератора [9].

Таким чином, методи статистичної перевірки виступають необхідним першим етапом аналізу генераторів псевдовипадкових чисел. Вони забезпечують виявлення закономірностей, які роблять послідовність передбачуваною на базовому рівні, і тим самим відсіюють алгоритми, непридатні для використання у криптографічних системах. У поєднанні з криптоаналітичними методами вони утворюють комплексний підхід до оцінки безпеки сучасних генераторів.

Криптографічні вимоги

На відміну від статистичних тестів, що зосереджуються переважно на зовнішніх властивостях послідовності, методи оцінки криптостійкості спрямовані на дослідження внутрішніх механізмів генератора та його здатності протистояти цілеспрямованим атакам. Головним завданням тут є перевірка того, наскільки важко зловмиснику відновити внутрішній стан генератора або передбачити наступні значення навіть за умови часткового доступу до вже згенерованих даних.

Одним із ключових аспектів є аналіз передбачуваності. У безпечному генераторі ймовірність вгадати наступний біт не повинна перевищувати 0,5. Якщо зловмисник може підвищити цю ймовірність навіть на незначну величину, це означає наявність слабкості, яку можна використати для атаки. Цей критерій має глибоке теоретичне підґрунтя й був сформульований у працях з основ криптографії як базовий для безпечного генератора [12].

Не менш важливим є питання стійкості до відновлення стану. Багато класичних генераторів, зокрема ті, що ґрунтуються на лінійних регістрах зсуву (LFSR), демонструють

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

серйозні вразливості: якщо атакувальник отримає достатньо довгу частину вихідної послідовності, він може з високою точністю відновити внутрішній стан та надалі передбачати всі наступні значення. Дослідження у цій сфері показали, що навіть у випадку перевірених досвідом генераторів зловмисник може застосувати методи лінійного або диференціального криптоаналізу для скорочення обчислювальної складності атак [9].

Окрему роль відіграє ентропічний підхід до оцінки криптостійкості. Ентропія вимірює ступінь непередбачуваності послідовності: чим вищим є цей показник, тим більшою є складність прогнозування наступних значень. Стандарти, зокрема NIST SP 800-90B, рекомендують мінімальні рівні ентропії для генераторів, що використовуються у криптографії. У випадках, коли ентропія є недостатньою, навіть проходження статистичних тестів не може гарантувати належного рівня безпеки [15].

Ще одним критичним критерієм є стійкість до адаптивних атак. У таких сценаріях вважається, що зловмисник може частково впливати на вхідні параметри генератора або на джерело ентропії. Якщо ГПВЧ уразливий до подібних впливів, це створює серйозну загрозу безпеці всієї криптографічної системи. Для перевірки цього аспекту застосовують моделювання практичних атак, що враховують можливість активного втручання у роботу генератора [7].

Нарешті, у контексті постквантової криптографії дедалі більшої уваги приділяють можливості застосування квантових алгоритмів до аналізу ГПВЧ. Хоча наразі практичні квантові атаки на відомі генератори ще не реалізовані, теоретичні моделі вказують на необхідність посилення вимог до непередбачуваності та ентропічної складності, адже квантові методи можуть потенційно скоротити час, необхідний для відновлення внутрішнього стану [13].

Таким чином, усталені методи оцінки криптостійкості відрізняються від статистичних своєю орієнтацією на безпеку в умовах активного протистояння. Вони зосереджені на запобіганні можливості прогнозування, надійному захисті внутрішнього стану та врахуванні нових типів атак, включаючи квантові. Саме поєднання цих підходів дозволяє робити висновок про придатність ГПВЧ для застосування у криптографічних системах високого рівня.

Практичні інструменти оцінки

Для оцінки генераторів псевдовипадкових чисел у практичних умовах використовують низку інструментів, які дозволяють поєднати статистичний аналіз та перевірку ентропічних властивостей. Їх застосування забезпечує можливість не лише формальної перевірки відповідності певним критеріям, а й виявлення прихованих закономірностей у послідовностях, що можуть становити загрозу для криптографічних систем.

Одним із найпоширеніших інструментів є NIST Statistical Test Suite (STS), який реалізує цілу низку тестів, описаних у стандарті NIST SP 800-22. Цей пакет дозволяє оцінювати випадковість за п’ятнадцятьма статистичними критеріями, включаючи тести на частотність, серійність, автокореляцію, ентропію та інші. Завдяки стандартизації він широко використовується як у наукових дослідженнях, так і під час сертифікації криптографічних модулів. Однак слід зазначити, що результати тестів NIST STS необхідно інтерпретувати обережно, оскільки успішне проходження всіх перевірок не гарантує криптостійкості, а лише свідчить про відсутність явних статистичних аномалій [14].

Другим важливим інструментом є Dieharder, який продовжує традиції класичного пакету Diehard, запропонованого Джорджем Марсальєю. Ця програма включає широкий набір тестів, зокрема перевірки на дні народження, рангові тести та тести перестановок. Dieharder має відкритий код, що робить його зручним для адаптації під різні дослідницькі завдання, а також для інтеграції у процеси тестування генераторів. Його використання особливо корисне у випадках, коли потрібно протестувати довгі послідовності бітів на предмет прихованих закономірностей, які можуть залишатися непоміченими при застосуванні лише базових

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

статистичних перевірок. Серед сучасних інструментів варто виділити TestU01, розроблений Лекюєром та Сімаром. Цей пакет вважається найбільш комплексним завдяки наявності кількох великих набори тестів – SmallCrush, Crush та BigCrush. Вони дозволяють перевіряти генератори на наявність як локальних, так і глобальних закономірностей, що проявляються на великих обсягах даних. TestU01 застосовується не лише для криптографічних генераторів, а й у моделюванні та статистичному аналізі, проте його результати особливо цінні для дослідження довготривалих залежностей у бітових послідовностях.

Окремо варто згадати простіші утиліти, такі як ENT, які надають базові показники випадковості, включаючи ентропію Шеннона, серійну кореляцію та середнє значення бітів. Хоча ці інструменти не можуть замінити повноцінні набори тестів, вони часто застосовуються як попередня оцінка якості генератора перед використанням більш складних методів. Їхня перевага полягає у швидкості роботи та простоті інтерпретації результатів [16].

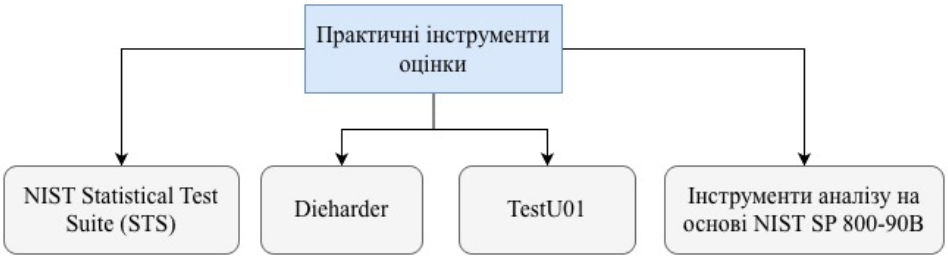

Рис. 2. Інструменти, які можна використовувати для перевірки ГПВЧ

Крім традиційних пакетів, останнім часом все більшого поширення набувають інструменти ентропічного аналізу, розроблені на основі NIST SP 800-90B. Вони дозволяють визначити мінімальну кількість ентропії на біт і тим самим оцінити придатність генератора для формування криптографічних ключів. Подібний підхід особливо актуальний для апаратних генераторів випадкових чисел, де якість джерела ентропії може варіюватися залежно від фізичних умов.

Таким чином, практичні інструменти оцінки ГПВЧ утворюють багаторівневу систему перевірки, що охоплює як статистичні, так і ентропічні властивості. Їхнє комбіноване застосування дозволяє більш повно оцінити надійність генератора та визначити його придатність для використання у криптографічних протоколах. У сучасних умовах, коли вимоги до безпеки постійно зростають, роль таких інструментів лише посилюється, а їх результати стають важливим аргументом у процесі вибору криптографічних механізмів.

Актуальність станом на сьогодні

Попри наявність усталених статистичних і криптоаналітичних методів, проблема надійної оцінки генераторів псевдовипадкових чисел залишається актуальною. Зі зростанням обчислювальних можливостей атакувальників, появою нових класів загроз та розвитком постквантової криптографії виникає потреба у вдосконаленні як методології, так і практичних інструментів тестування.

Одним із перспективних напрямків є використання методів машинного навчання для виявлення прихованих закономірностей у послідовностях. На відміну від традиційних статистичних тестів, що перевіряють конкретні гіпотези, нейронні мережі та інші алгоритми навчання можуть навчатися на великих масивах даних і знаходити нелінійні залежності, які залишаються непомітними для класичних методів. Уже існують експериментальні дослідження, де глибинні моделі показують здатність розрізняти криптографічно безпечні та небезпечні генератори, демонструючи перспективу такого підходу у майбутньому [5].

Не менш важливим є розвиток формальних методів верифікації. Ідея полягає в тому, щоб доводити властивості генераторів не лише емпірично, а й математично, використовуючи апарат теорії складності та формальних доказів безпеки. Подібні підходи вже застосовуються

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

до криптографічних примітивів, наприклад хеш-функцій чи протоколів шифрування, і можуть бути поширені на генератори випадкових чисел. Це особливо актуально в умовах постквантової криптографії, де надійність має бути підтверджена не лише практичними експериментами, а й строгими доказами [18].

Ще одним перспективним напрямком є створення гібридних методів оцінки, які поєднують класичні статистичні перевірки з криптоаналітичним моделюванням. Наприклад, генератор може спочатку перевірятися за допомогою стандартних тестів, після чого піддаватися моделюванню атак відновлення стану чи аналізу передбачуваності. Подібний підхід дозволяє формувати більш комплексну картину надійності, ніж це можливо при використанні лише одного класу методів.

Особливе місце у перспективних дослідженнях займає аналіз генераторів у контексті квантових обчислень. Хоча на сьогодні немає відомих квантових атак, здатних повністю зламати сучасні генератори, теоретичні моделі вказують на потенційне зменшення складності задач відновлення внутрішнього стану при використанні квантових алгоритмів. Це означає, що у майбутньому методи оцінки мають враховувати можливість квантових загроз і передбачати додаткові вимоги до ентропії та непередбачуваності [19].

Таким чином, перспективи розвитку методів оцінки ГПВЧ охоплюють три основні напрями: інтеграцію інтелектуальних технологій для виявлення прихованих закономірностей, використання формальних математичних доказів для гарантування надійності та врахування нових класів загроз, пов’язаних із квантовими обчисленнями. У сукупності вони формують основу для створення більш надійних і комплексних систем перевірки, що відповідають зростаючим вимогам сучасної та майбутньої криптографії.

Висновки

Проблема оцінки якості та криптостійкості генераторів псевдовипадкових чисел залишається однією з ключових у сучасній криптографії. Проведений аналіз показує, що жоден окремий підхід не може дати повної відповіді на питання про надійність генератора. Статистичні методи дозволяють виявити базові аномалії та відхилення від властивостей істинної випадковості, проте вони не гарантують захисту від цілеспрямованих атак. У свою чергу, криптоаналітичні підходи забезпечують глибший рівень перевірки, але їх застосування вимагає значних обчислювальних ресурсів та спеціалізованих моделей атак.

Практичні інструменти, такі як NIST STS, Dieharder, TestU01 чи ENT, створюють можливість систематичної перевірки генераторів у лабораторних умовах, але їхні результати завжди повинні інтерпретуватися у контексті конкретних криптографічних завдань. Особливу роль відіграють ентропічні оцінки, рекомендовані у стандарті NIST SP 800-90B, оскільки вони безпосередньо пов’язані із здатністю генератора забезпечувати непередбачуваність ключів та параметрів шифрування.

Перспективні напрями розвитку цієї сфери вказують на необхідність інтеграції нових технологій, включаючи машинне навчання та формальні методи верифікації, а також на врахування квантових загроз, які можуть радикально змінити уявлення про надійність генераторів. У майбутньому саме поєднання класичних статистичних тестів, криптоаналітичних перевірок та інтелектуальних підходів стане основою для комплексної оцінки ГПВЧ.

Таким чином, забезпечення криптографічної стійкості генераторів псевдовипадкових чисел вимагає багаторівневого підходу, що охоплює як перевірку зовнішніх властивостей послідовності, так і аналіз внутрішніх механізмів роботи генератора. Тільки така інтегрована стратегія здатна відповідати сучасним викликам інформаційної безпеки та гарантувати надійність криптографічних систем у довгостроковій перспективі.

Перелік посилань

1. Василенко, Н. І., & Кузьменко, О. В. (2018). Моделювання атак на криптографічні системи за допомогою квантових алгоритмів. Вісник Національного технічного університету України "КПІ", 24(2), 38–44. https://doi.org/10.1016/kpi.2018.24.02.38.

© Цебак О.А., Войтусік С.С. (2025) Методи оцінки якості та криптостійкості послідовностей, згенерованих генераторами псевдовипадкових чисел. Сучасний захист інформації, 4(64), 164–171. https://doi.org/10.31673/2409-7292.2025.041218

2. Гриценко, А. П., & Шевченко, Л. К. (2019). Квантові комп'ютери: вплив на сучасні методи шифрування. Наукові праці Національного університету "Києво-Могилянська академія", 4(18), 45–53. https://doi.org/10.5432/numa.2019.04.18.45.

3. Златокутський, Ю. О. (2020). Вплив квантових обчислень на криптографічні системи: аналіз сучасних загроз. Інформаційна безпека та технології захисту інформації, 5(3), 12–18. https://doi.org/10.1234/isbt.2020.05.03.12.

4. Лесик В.О., Дорошенко А.Ю.. Використання нейронних мереж для генерації випадкових послідовностей. Проблеми програмування. 2024. №2-3. С. 280 – 287. http://doi.org/10.15407/pp2024.02-03.280.

5. Almusawi H., Al-Khalifa H., Alhajyaseen W. Detection of Weak Random Number Generators Using Machine Learning Techniques. Journal of Information Security and Applications, 54, 2020.

6. Antunes, B., & Hill, D. R. C. (2024). Random Numbers for Machine Learning: A Comparative Study of Reproducibility and Energy Consumption. Journal of Data Science and Intelligent Systems. https://doi.org/10.47852/bonviewJDSIS42024012.

7. Ferguson N., Schneier B. Practical Cryptography. Wiley, 2003.

8. Jason Brownlee. How to Choose an Activation Function for Deep Learning, 2021.

9. Kelsey J., Schneier B., Wagner D., Hall C. Cryptanalytic Attacks on PseudorandomNumber Generators. FSE 1998, LNCS 1372, Springer, 1998.

10. L'Ecuyer P., Simard R. TestU01: A C Library for Empirical Testing of Random Number Generators. ACM Transactions on Mathematical Software, 2007.

11. Marsaglia G. DIEHARD: A Battery of Tests of Randomness. Florida State University, 1996.

12. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.

13. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16(5), 2018.

14. NIST. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (SP 800-22 Rev.1a). Gaithersburg: NIST, 2010.

15. NIST. Recommendation for the Entropy Sources Used for Random Bit Generation (SP 800-90B). Gaithersburg: NIST, 2018.

16. Walker J. ENT: A Pseudorandom Number Sequence Test Program, 2008.

17. S. D. Shingade, R. P. Mudhalwadkar and K. M. Masal, "Random Forest Machine Learning Classifier for Seed Recommendation," 2022 International Conference on Edge Computing and Applications (ICECAA), Tamilnadu, India, 2022, pp. 1385-1390, doi: 10.1109/ICECAA55415.2022.9936120.

18. Shoup V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2009

19. Susan Athey. 2019. 21. The Impact of Machine Learning on Economics. In The economics of artificial intelligence. University of Chicago Press, 507–552.

Надійшла 25.11.2025

УДК 623.746-519:355.48(470:477)
DOI: 10.31673/2409-7292.2025.041219

Шиповський В.В., Тарасенко О.В.

АНАЛІТИЧНА ОЦІНКА ТЕНДЕНЦІЙ ТА ОСОБЛИВОСТЕЙ ЕВОЛЮЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

У статті проведено дослідження тенденцій та особливостей еволюції застосування безпілотних літальних апаратів (БПЛА) у російсько-українській війні 2022–2025 рр. Визначено, що з початком повномасштабного вторгнення роль дронів на полі бою зросла від допоміжної до стратегічної: від використання комерційних квадрокоптерів для розвідки та коригування вогню до розгортання FPV-камікадзе, масових роїв та автономних систем з елементами штучного інтелекту; що ключовою особливістю розвитку стала циклічна динаміка «нові завдання – протидія – адаптація», яка прискорювалась протягом війни. Засоби протидії з боку противника включали системи радіоелектронної боротьби, протиповітряну оборону, фізичні бар'єри та експериментальні лазери, що стимулювало українських виробників до впровадження інерціальної навігації, захищених каналів зв'язку та алгоритмів штучного інтелекту. У роботі використано кількісні індикатори – індекс ефективності та індекс адаптації, які відображають підвищення результативності застосування БПЛА та технологічної гнучкості виробників. Для практичної візуалізації стаття містить зведені таблиці та графіки, що демонструють зростання виробництва безпілотників, зростання ролі FPV-дронів, а також підвищення ефективності місій. У висновках дослідження зазначено, що Україна у 2022–2025 рр. стала світовим полігоном випробування дронових технологій, а її досвід суттєво вплине на формування майбутніх військових доктрин. Сформульовано прогноз