КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1220
УДК 004.021:519.217

Гришанович Тетяна Олександрівна
кандидат фізико-математичних наук, доцент
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID: 0000-0002-3595-6964
Hryshanovych.Tatiana@vnu.edu.ua

Андрощук Яна Вікторівна
здобувачка освіти
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID: 0009-0001-7905-4962
Androshchuk.Yana2023@vnu.edu.ua

Ярмольська Яна Сергіївна
здобувачка освіти
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID: 0009-0007-0234-8640
Yarmolska.Yana2023@vnu.edu.ua

ПОРІВНЯЛЬНИЙ АНАЛІЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ТА ЇХ ОЦІНКА

Анотація. У статті досліджено особливості функціонування генераторів псевдовипадкових послідовностей як ключового компонента сучасних інформаційних систем, що застосовуються в моделюванні, криптографії, обробці даних та тестуванні програмного забезпечення. Основну увагу приділено порівняльному аналізу чотирьох підходів до генерування: лінійного конгруентного генератора, методу середніх квадратів, генератора Mersenne Twister та генератора на основі криптографічного хешування. У межах дослідження розроблено програмний засіб, який дозволяє моделювати роботу зазначених генераторів і здійснювати їх комплексне оцінювання за допомогою статистичних та візуальних методів аналізу. Для визначення якості псевдовипадкових послідовностей використано критерій узгодженості Пірсона, оцінювання дисперсії та аналіз автокореляційних залежностей. Отримані результати подано у вигляді гістограм розподілу та графіків, що забезпечує наочне відображення рівномірності розподілу, ступеня випадковості та наявності можливих закономірностей у згенерованих даних. Проведений аналіз показав, що генератор Mersenne Twister і криптографічні генератори демонструють найкращі статистичні характеристики, зокрема близькість до теоретичних значень, низький рівень автокореляції та високу рівномірність розподілу. Встановлено, що лінійний конгруентний генератор може забезпечувати задовільні результати лише за умови коректного підбору параметрів, тоді як метод середніх квадратів характеризується швидким виродженням послідовності та низькою якістю генерування. Отримані результати підтверджують необхідність обґрунтованого вибору генератора залежно від сфери застосування та вимог до статистичних і криптографічних властивостей. Запропонований підхід до комплексного аналізу може бути використаний у навчальних і прикладних задачах для оцінювання ефективності генераторів псевдовипадкових чисел.

Ключові слова: псевдовипадкові числа; алгоритми генерування; генератор Mersenne Twister; лінійний конгруентний генератор; статистичний аналіз; автокореляція; критерій Пірсона.

ВСТУП

Псевдовипадкова послідовність – це послідовність, що виглядає як випадкова, але насправді має скінченний період повторення. Генерування псевдовипадкових послідовностей і перевірка на випадковість згенерованої послідовності є одними з найважливіших проблем сучасної криптології.

Генератор псевдовипадкових чисел (ГПСЧ, англ. Pseudorandom number generator, PRNG) – алгоритм, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підкоряються заданому розподілу (зазвичай рівномірному). [2] Генератори псевдовипадкових послідовностей є важливим інструментом в числових методах, криптографії, ігровій індустрії та тестуванні програмного забезпечення. Вони використовуються для генерування чисел, що за статистичними властивостями схожі на випадкові, і відіграють критичну роль в моделюванні випадкових процесів, шифруванні даних та верифікації програмних продуктів. У криптографії генератори псевдовипадкових послідовностей використовуються для створення ключів, ініціалізаційних векторів, одноразових кодів та інших елементів захисту, тому недостатня якість генератора може стати причиною зниження рівня безпеки всієї системи. У задачах моделювання, зокрема при застосуванні методу Монте-Карло, псевдовипадкові числа визначають точність відтворення процесів і достовірність отриманих результатів. У сфері тестування програмного забезпечення генератори застосовуються для автоматичного формування вхідних даних, сценаріїв навантаження, перевірки граничних випадків і виявлення прихованих дефектів. Оскільки різні типи генераторів можуть значно відрізнятися за своїми властивостями та ефективністю, порівняльний аналіз цих алгоритмів є актуальним для вибору оптимальних методів у конкретних сферах застосування. За таких умов особливо важливим є обґрунтований вибір генератора, який поєднує належні статистичні характеристики, ефективність роботи та відповідність вимогам конкретної прикладної галузі.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях генераторів псевдовипадкових послідовностей основна увага зосереджується на трьох взаємопов'язаних напрямах: розробленні ефективних алгоритмів генерування, статистичному оцінюванні якості згенерованих послідовностей та визначенні придатності конкретних генераторів до використання у криптографії, моделюванні й програмній інженерії. У науковій літературі підкреслюється, що універсального генератора, однаково ефективного для всіх прикладних задач, не існує, оскільки вимоги до випадковості, швидкодії та передбачуваності суттєво залежать від сфери застосування. Зокрема, для імітаційного моделювання ключовими є довгий період, рівномірність розподілу та низька корельованість, тоді як у криптографічних застосуваннях визначальними стають непередбачуваність, правильна початкова ініціалізація та стійкість до відновлення внутрішнього стану генератора [7].

Класичним етапом у розвитку теорії генераторів псевдовипадкових чисел стала поява алгоритму **Mersenne Twister**, запропонованого М. Мацумото та Т. Нішімурою [9]. Цей генератор набув широкого поширення завдяки дуже великому періоду та добрим властивостям рівномірності у багатовимірному просторі, тому тривалий час розглядався як один із базових стандартів для задач статистичного моделювання. Водночас у подальших роботах було показано, що попри високі статистичні характеристики для некриптографічних задач, такі генератори не забезпечують вимог криптографічної стійкості, оскільки їхній внутрішній стан у принципі може бути відновлений за достатньої кількості вихідних значень.

Помітне місце в наукових публікаціях посідають дослідження швидких компактних генераторів сімейства XORSHIFT, запропонованих Дж. Марсальєю [8]. Їхня популярність пояснюється простою структурою, високою швидкодією та низькими обчислювальними витратами, що робить такі алгоритми привабливими для вбудованих систем, симуляцій і задач, де критичною є продуктивність. Разом із тим у літературі наголошується, що простота XORSHIFT-генераторів не завжди гарантує достатню якість для всіх сценаріїв використання, а тому їх доцільно оцінювати за допомогою статистичних тестів і розглядати переважно як інструмент для прикладних, а не криптографічних цілей [1].

У новіших дослідженнях значну увагу приділено сімейству PCG (Permuted Congruential Generator), яке позиціонується як поєднання простоти, швидкодії, компактності реалізації та належної статистичної якості. У роботі М. О'Нілл [10] показано, що генератори цього типу можуть демонструвати кращий баланс між продуктивністю та статистичними властивостями порівняно з частиною традиційних рішень, особливо в прикладному програмуванні. Саме тому сучасні порівняльні дослідження дедалі частіше включають не лише класичні LCG, Mersenne Twister чи XORSHIFT, а й новіші генератори, орієнтовані на практичне використання в програмних системах [3], [11].

Окремий напрям досліджень пов'язаний із криптографічними генераторами псевдовипадкових бітів [2]. У цьому контексті ключове значення мають документи NIST серії SP 800-90A, у яких визначено рекомендовані механізми детермінованих генераторів випадкових бітів на основі криптографічних хеш-функцій, HMAC і блокових шифрів. Ці публікації фактично закріплюють підхід, за яким оцінювання генератора для криптографії не може обмежуватися лише перевіркою статистичних властивостей; воно має враховувати наявність ентропії, процедури ініціалізації, повторного засіву та захищеність внутрішнього стану. Отже, у сучасних дослідженнях чітко простежується розмежування між генераторами для загального призначення та генераторами для криптографічних застосувань [4].

Важливе місце в наукових публікаціях займають і праці, присвячені статистичному тестуванню випадкових і псевдовипадкових послідовностей [5]. Одним із найвідоміших підходів є тестовий набір

NISTSP800-22Rev.1a [6], який використовується для аналізу частоти бітів, серій, шаблонів, ентропійних характеристик, лінійної складності та інших параметрів послідовностей. У цих дослідженнях наголошується, що проходження окремих статистичних тестів не є достатньою умовою придатності генератора для криптографії, однак є важливим етапом первинного оцінювання його якості. Саме тому сучасні порівняльні роботи зазвичай поєднують аналіз теоретичних властивостей алгоритмів із практичним тестуванням згенерованих послідовностей.

Узагальнення наявних публікацій дає підстави стверджувати, що більшість авторів розглядають генератори псевдовипадкових послідовностей не ізольовано, а в контексті конкретних прикладних завдань. При цьому в літературі достатньо добре висвітлено математичні основи окремих генераторів і підходи до їх статистичного тестування, однак потребують подальшого опрацювання питання комплексного порівняння алгоритмів одночасно за критеріями статистичної якості, швидкодії та практичної придатності до використання у криптографії, моделюванні та тестуванні програмного забезпечення. Саме ця обставина зумовлює доцільність проведення порівняльного аналізу генераторів псевдовипадкових послідовностей у межах даної статті.

Мета статті. Мета цієї роботи полягає у дослідженні особливостей функціонування генераторів псевдовипадкових послідовностей, зокрема лінійного конгруентного генератора (LCG) та генератора Mersenne Twister (MT19937), криптографічного хешу та методу середніх квадратів проведенні їх порівняльного аналізу за критеріями статистичної якості, швидкодії та практичної придатності, а також у формуванні рекомендацій щодо вибору генератора залежно від сфери застосування.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах проведеного дослідження було реалізовано програмний засіб, призначений для моделювання роботи генераторів псевдовипадкових чисел (лінійний конгруентний генератор (LCG), метод середніх квадратів, розподіл Mersenne Twister та криптографічний хеш) та їх комплексного аналізу на основі візуальних і статистичних характеристик. Згідно з представленими результатами, програма формує вибірки псевдовипадкових значень та відображає їх у вигляді гістограм розподілу та графіків послідовностей, що дає змогу оцінити рівномірність розподілу, наявність кореляційних залежностей і загальний рівень випадковості.

Для кількісного оцінювання якості згенерованих послідовностей використано класичні статистичні характеристики, зокрема критерій узгодженості Пірсона, дисперсію та коефіцієнт автокореляції.

Перевірка рівномірності розподілу здійснюється за допомогою критерію Пірсона:

$$X^2 = \sum_{i=1}^{k} \frac{(n_i - np_i)^2}{np_i},$$

де n_i – кількість значень у i-му інтервалі,
n – обсяг вибірки,
p_i – теоретична ймовірність потрапляння у відповідний інтервал (для рівномірного розподілу $p_i = \frac{1}{k}$),
k – кількість інтервалів.

Для якісних генераторів значення статистики X^2 повинно належати допустимому інтервалу, визначеному критичними значеннями розподілу Пірсона.

Оцінювання розсіювання значень здійснюється за допомогою дисперсії:

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2$$

де $\overline{x}$ – середнє значення вибірки:

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i.$$

Для рівномірного розподілу на інтервалі [0, 1] теоретичне значення дисперсії становить:

$$\sigma^2 = \frac{1}{12} \approx 0.0833.$$

Для виявлення залежностей між елементами послідовності використовується коефіцієнт автокореляції:

$$\rho_k = \frac{\sum_{i=1}^{n-k}(x_i - \overline{x})(x_{i+k} - \overline{x})}{\sum_{i=1}^{n}(x_i - \overline{x})^2}$$

Використання критерію Пірсона зумовлене його ефективністю для перевірки відповідності

емпіричного розподілу теоретичному, що є ключовим при оцінюванні рівномірності псевдовипадкових послідовностей. Крім того, цей критерій є одним із найбільш поширених і статистично обґрунтованих методів, що дозволяє отримати надійні результати при порівнянні спостережуваних та очікуваних частот.

На рисунку 1 представлено гістограму розподілу, отриману за допомогою лінійного конгруентного генератора.

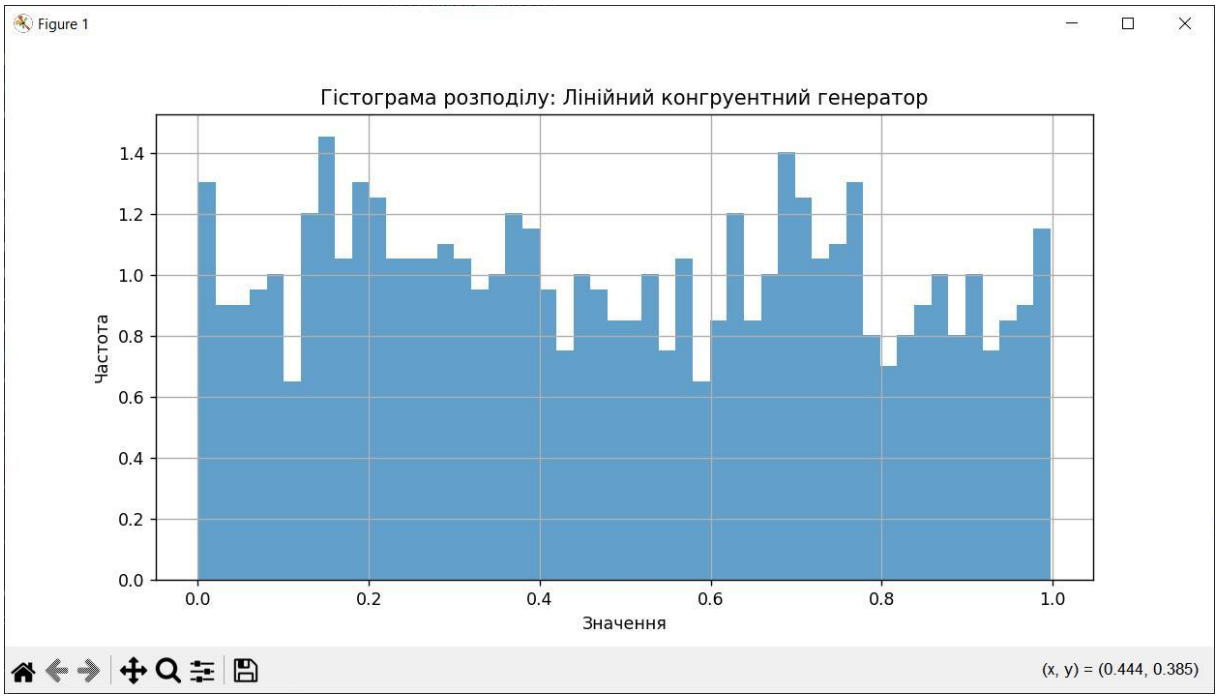

Рис. 1. Гістограма розподілу ЛКГ

На рисунку 2 наведено графік послідовності, згенерованої цим методом, який дозволяє оцінити наявність можливих залежностей між сусідніми значеннями.

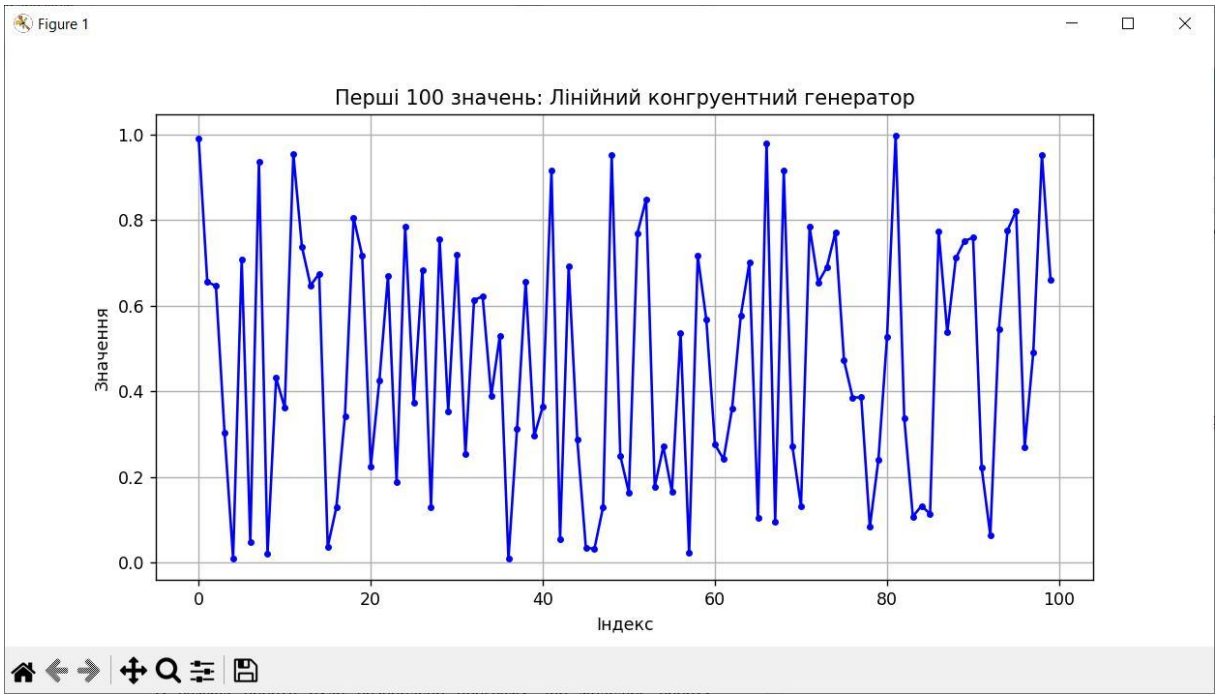

Рис. 2. Графік ЛКГ

Для методу середніх квадратів у програмі також передбачено побудову гістограм і графіків. Відповідні результати наведено на рисунках 3 та 4. Аналіз отриманих візуалізацій свідчить про нерівномірність розподілу значень та наявність повторюваних закономірностей у послідовності. Це підтверджує низьку якість генерування та схильність методу до швидкого виродження.

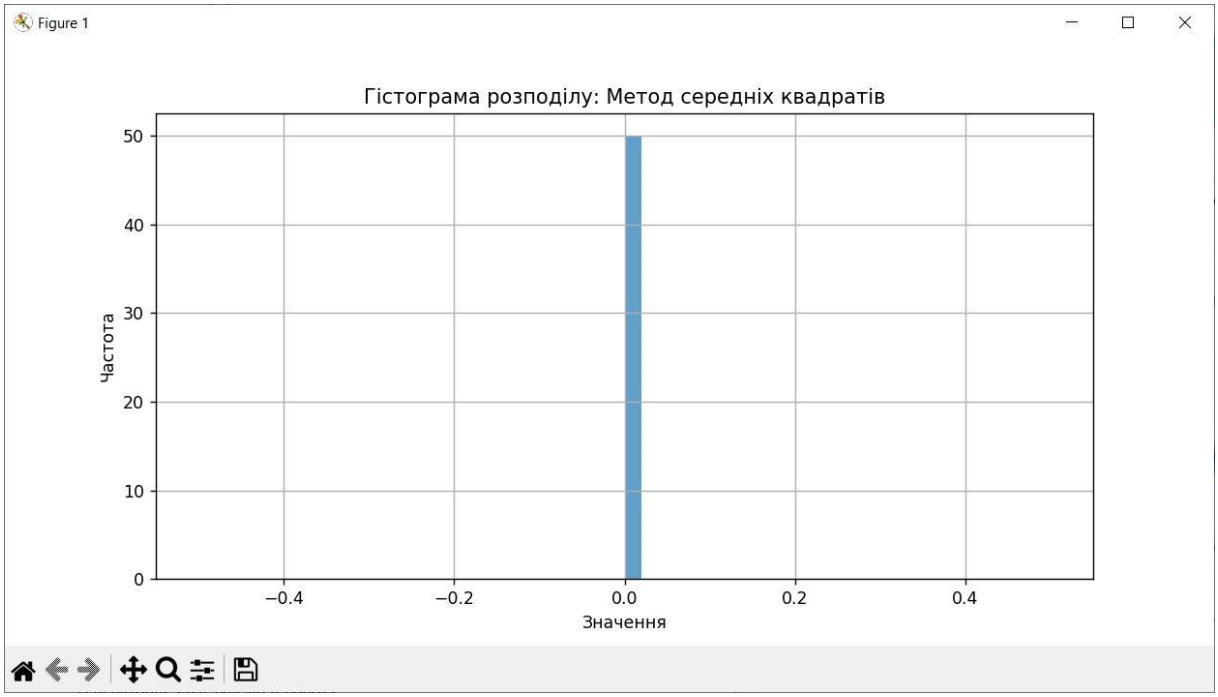

Рис. 3. Гістограма методу середніх квадратів

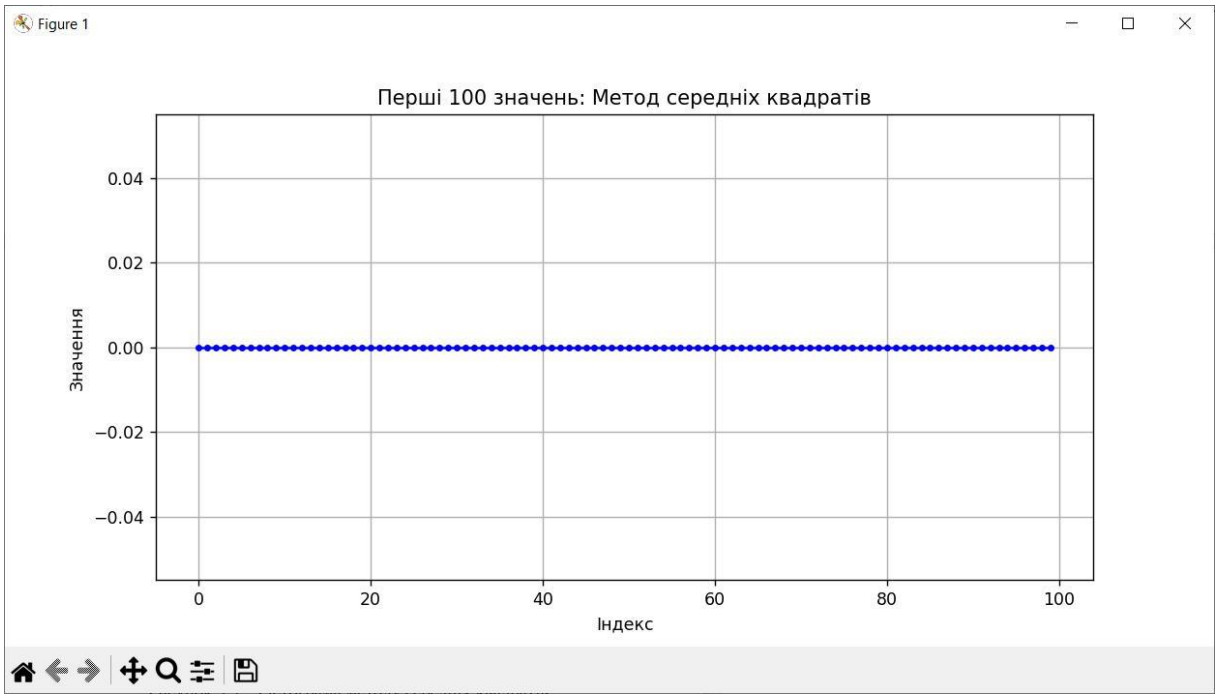

Рис. 4. Графік методу середніх квадратів

Аналогічно, для генератора Mersenne Twister реалізовано засоби візуалізації, що відображені на рисунках 5 та 6. Ці графічні представлення демонструють високу рівномірність розподілу та відсутність виражених закономірностей.

Гістограми мають майже рівномірний характер заповнення інтервалів, що свідчить про наближеність до теоретичного розподілу. Графіки послідовностей не виявляють періодичних структур або повторюваних шаблонів, що підтверджує високу якість генерації. Це дозволяє рекомендувати даний генератор для використання в задачах статистичного моделювання та обробки даних.

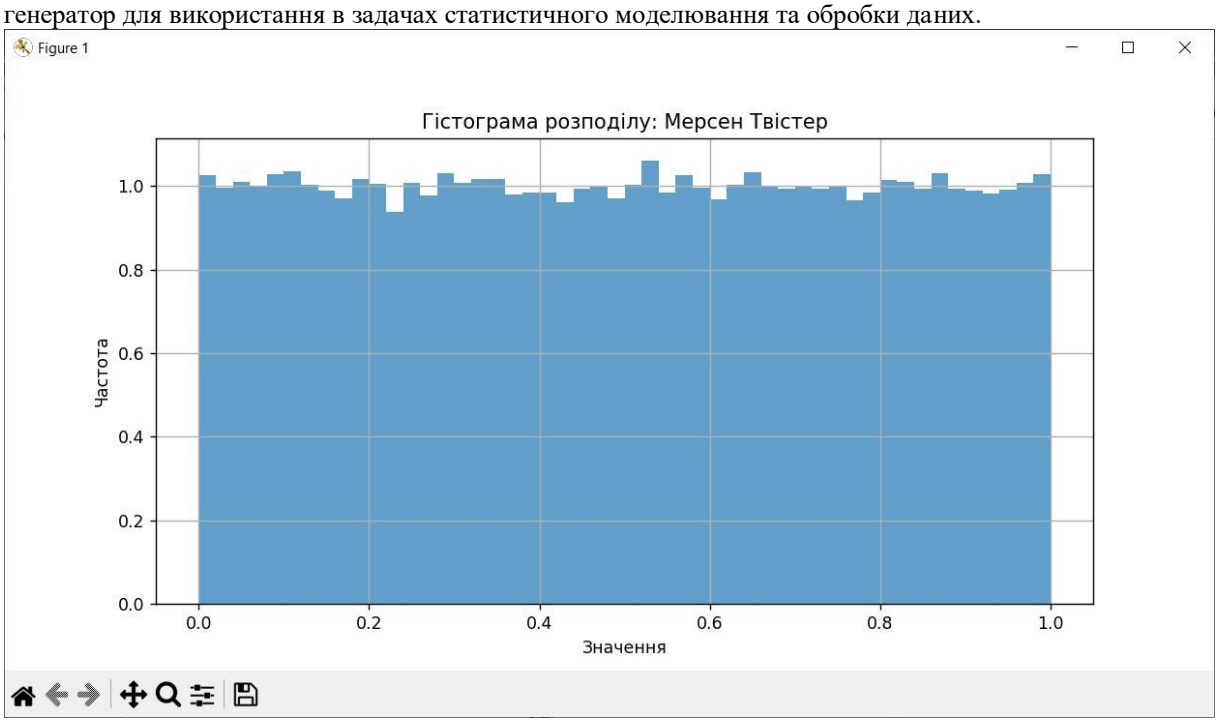

Рис. 5. Гістограма розподілу Mersenne Twister

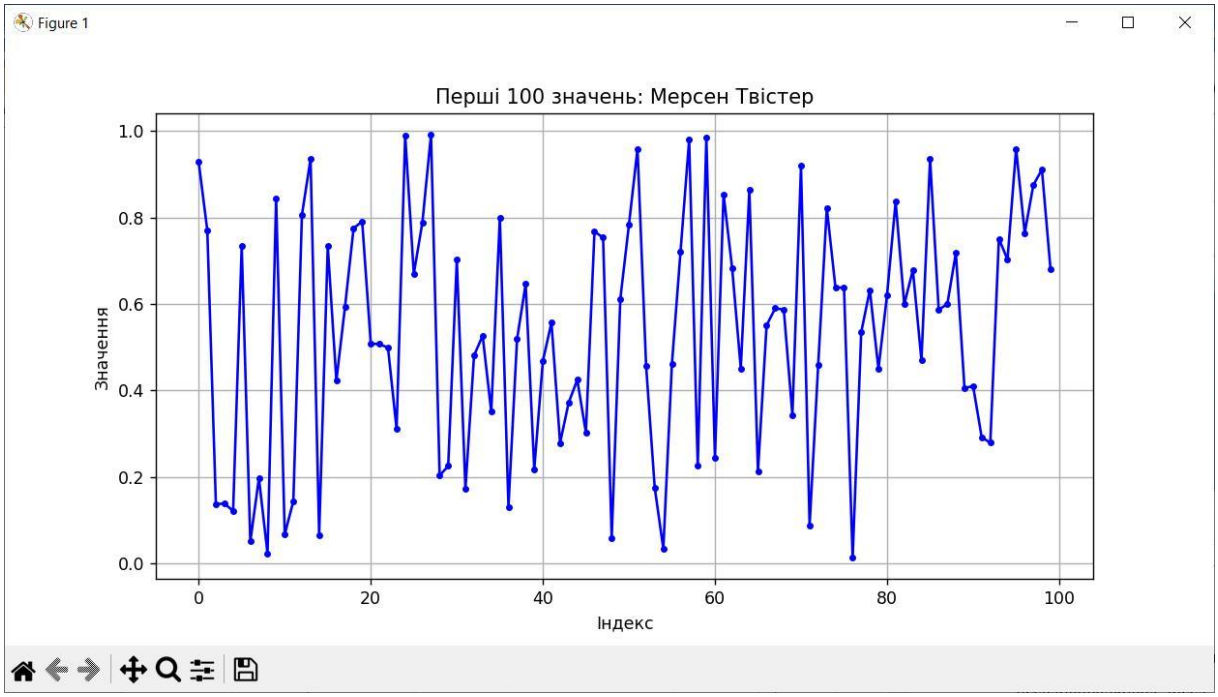

Рис. 6. Графік розподілу Mersenne Twister

Для генератора на основі криптографічного хешу результати подано у вигляді гістограми та графіка (рисунки 7 та 8), які свідчать про високий рівень випадковості та незалежності значень. Додатково спостерігається відсутність виражених піків або регулярних структур у розподілі, що підтверджує рівномірне заповнення інтервалів. Значення послідовності не демонструють помітних кореляційних залежностей, що є характерною ознакою якісного генератора. Отримані результати узгоджуються з

теоретичними властивостями криптографічних хеш-функцій, які забезпечують високу чутливість до змін вхідних даних. Таким чином, можна зробити висновок про придатність даного підходу для генерування псевдовипадкових послідовностей.

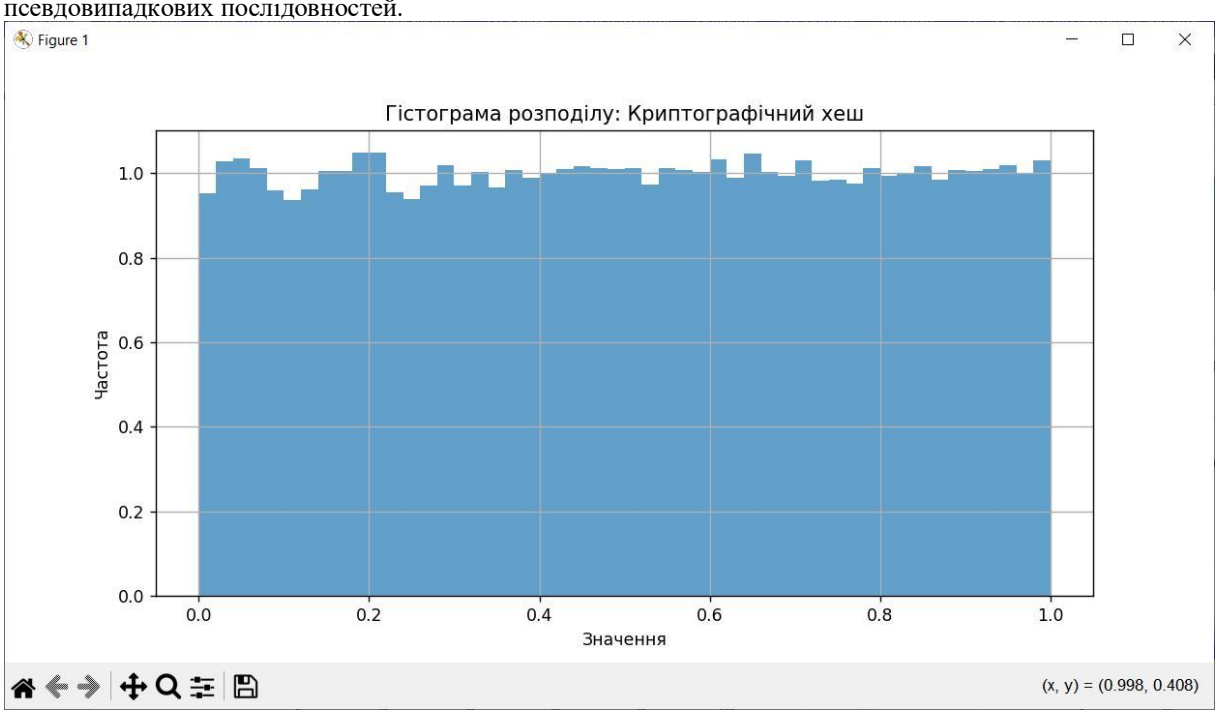

Рис. 7. Гістограма розподілу криптографічного хешу

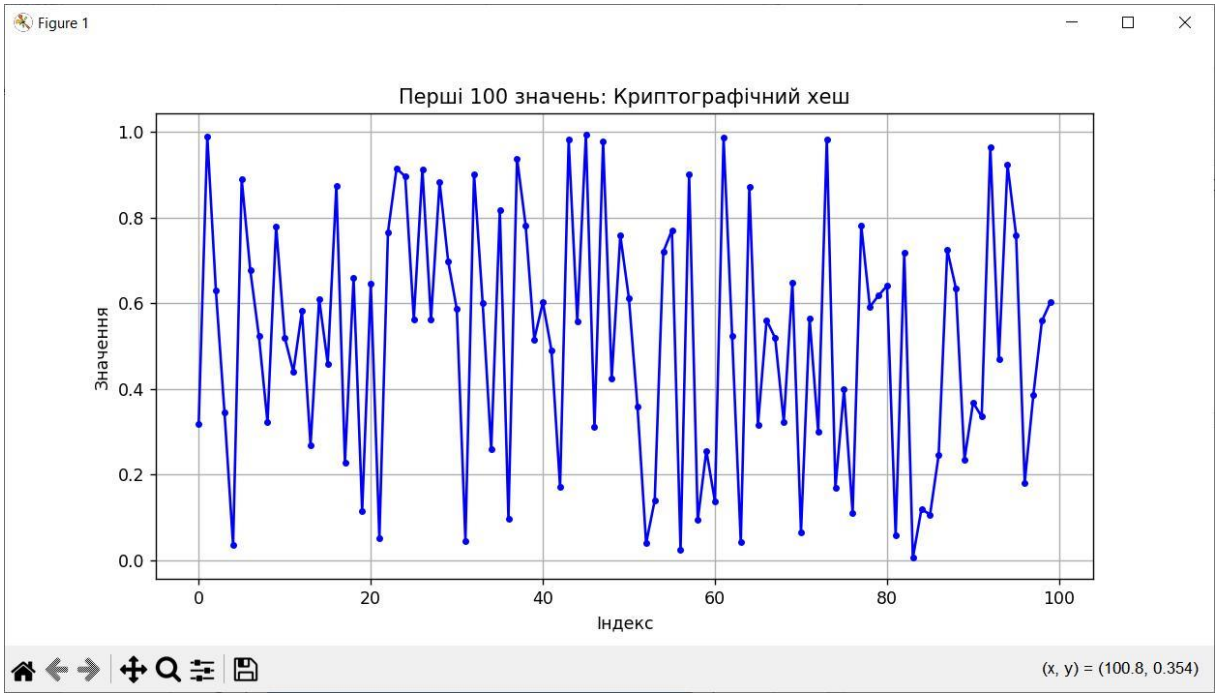

Рис. 8. Графік розподілу криптографічного хешу

Окремою функціональною можливістю програмного засобу є аналіз впливу параметрів генератора на якість результатів. Зокрема, для лінійного конгруентного генератора передбачено дослідження різних наборів параметрів, що ілюструється на рисунках 9–11. У програмі реалізовано порівняння результатів для наборів параметрів різної якості — поганих, середніх і оптимальних. Це дозволяє наочно простежити, як вибір параметрів впливає на рівномірність розподілу, значення статистичних характеристик та ступінь випадковості згенерованих послідовностей.

ISSN 2663 – 4023

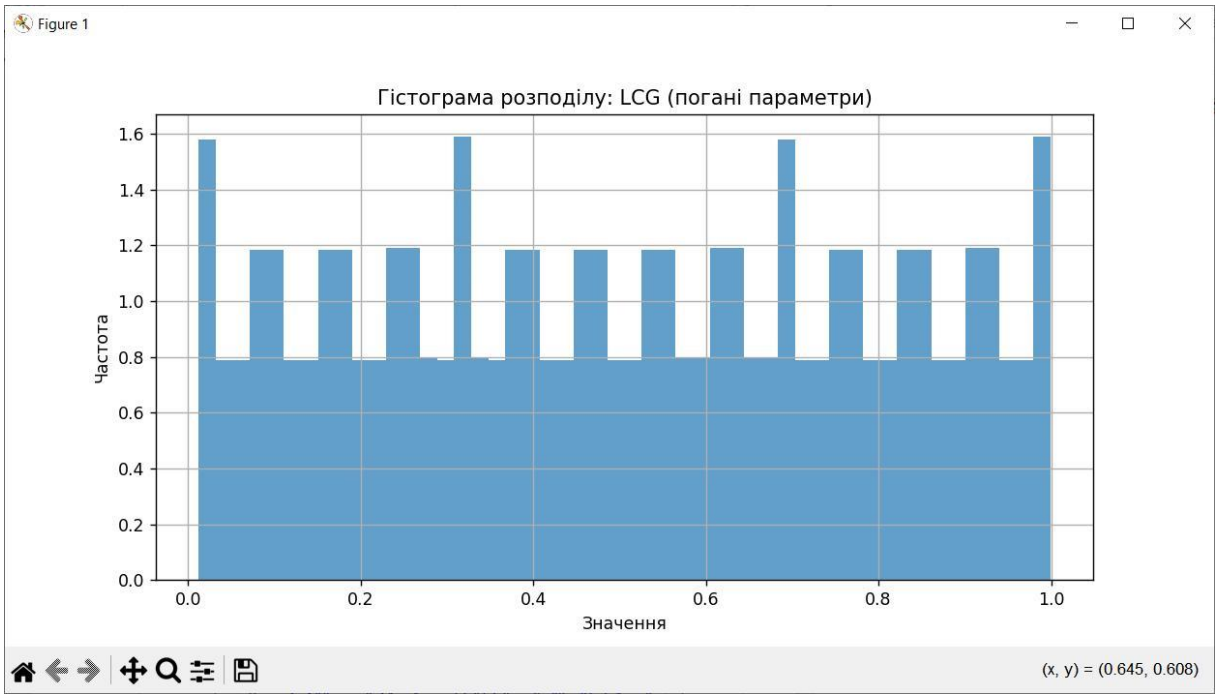

Рис. 9. Гістограма розподілу LCG (погані параметри)

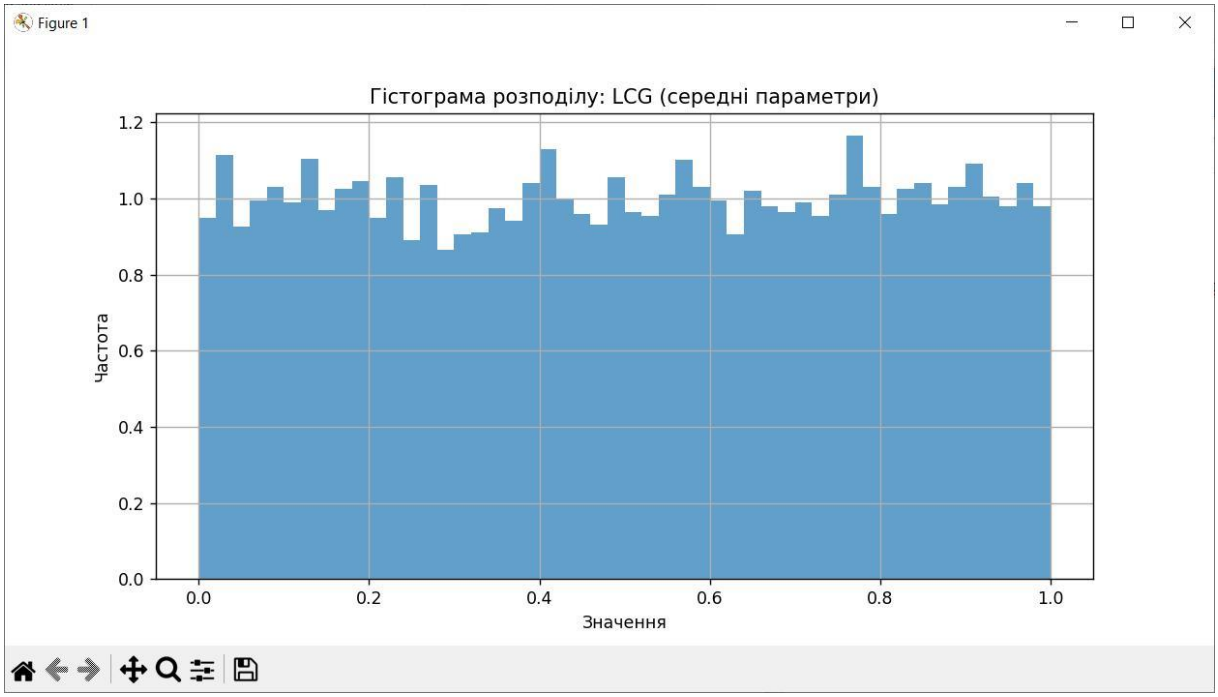

Рис. 10. Гістограма розподілу LCG (середні параметри)

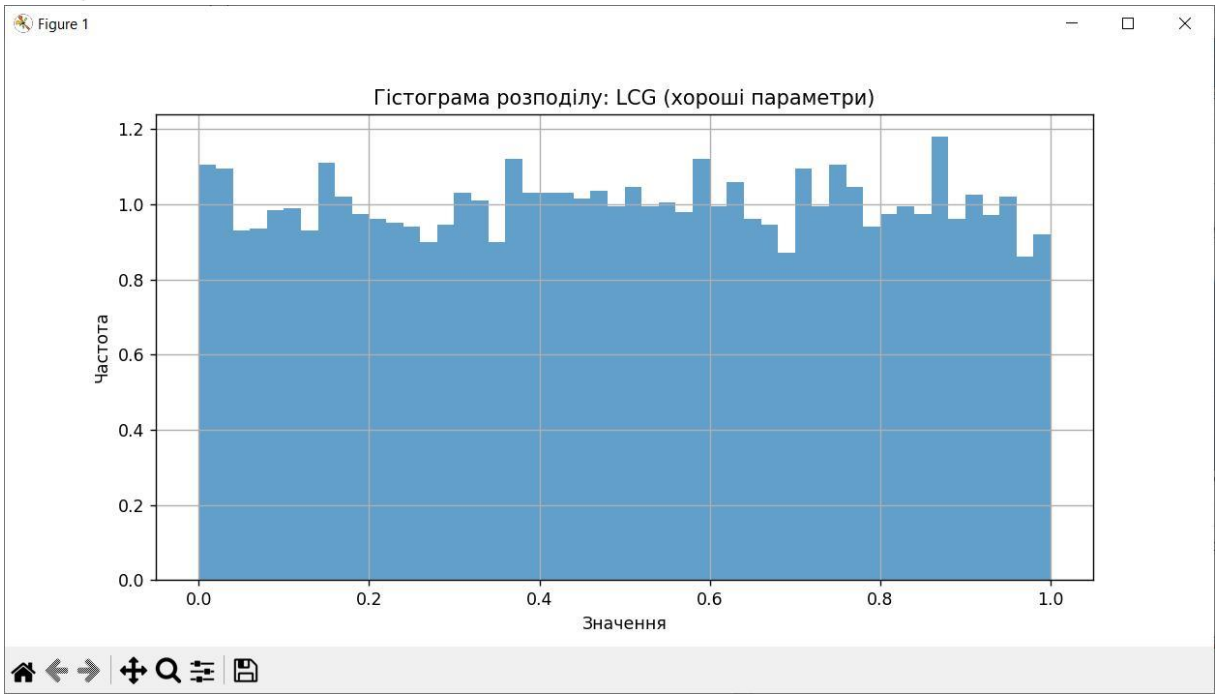

Рис. 11. Гістограма розподілу LCG (хороші параметри)

Як видно з рисунків, то програма детально проходить по кожному генератору та проводить тестування.

Функція обчислення статистики має вигляд:

```
def chi_square_test(data, bins=50):
    counts, _ = np.histogram(data, bins=bins, range=(0, 1))
    expected = np.ones(bins) * (len(data) / bins)
    chi2_stat, p_value = chisquare(counts, expected)
    return chi2_stat, p_value
```

Аналіз отриманих результатів показує, що генератор **Mersenne Twister** та генератор на основі криптографічного хешу демонструють значення статистики (X^2) у межах 8–15 (при ($k = 10$)), що відповідає рівномірному розподілу. Значення дисперсії для цих генераторів становить $\sigma^2 \approx 0.08 - 0.085$, що є близьким до теоретичного значення, а коефіцієнт автокореляції наближається до нуля, що свідчить про відсутність лінійних залежностей у послідовностях.

Для лінійного конгруентного генератора результати суттєво залежать від вибору параметрів. При оптимальних параметрах значення статистики (X^2) знаходиться в межах 15–20, дисперсія наближається до теоретичної, однак коефіцієнт автокореляції залишається на рівні $\rho \approx 0.05 - 0.1$, що свідчить про наявність слабких залежностей. При невдалому виборі параметрів спостерігається значне погіршення показників: (X^2) зростає до 40–60, дисперсія зменшується, а автокореляція перевищує 0.3, що вказує на виражену структурованість послідовності.

Метод середніх квадратів демонструє найгірші результати: значення (X^2) перевищує 30, дисперсія суттєво відрізняється від теоретичної, а коефіцієнт автокореляції є високим. Це свідчить про швидке виродження послідовності та її непридатність для практичного застосування.

Генератор на основі криптографічного хешу демонструє стабільні результати незалежно від початкових параметрів, що забезпечує високий рівень надійності генерування. Отримані значення статистичних показників свідчать про практичну відсутність кореляцій та високу рівномірність розподілу, що відповідає вимогам до криптографічно стійких генераторів. Завдяки цим властивостям такий підхід є доцільним для використання у задачах, де критичною є непередбачуваність і захищеність згенерованих даних.

Таблиця 1

Порівняльна характеристика генераторів

Генератор	χ^2 (k=10)	Дисперсія σ^2	Автокореляція ρ	Якість розподілу	Висновок
ЛКГ	15–25	0.075–0.085	0.1–0.3	Задовільна	Залежить від параметрів
Метод середніх квадратів	>30	<0.07	>0.3	Незадовільна	Непридатний
Генератор Mersenne Twister	8–15	0.08–0.085	≈0	Висока	Рекомендований для моделювання
Криптографічний хеш	8–15	0.08–0.085	≈0	Дуже висока	Придатний для криптографії
ЛКГ (погані параметри)	40–60	<0.07	>0.3	Низька	Не використовувати
ЛКГ (середні параметри)	20–30	~0.075	0.1–0.2	Середня	Обмежено
ЛКГ (хороші параметри)	15–20	~0.08	0.05–0.1	Вище середнього	Можливе використання

Отримані результати свідчать, що використання комплексного підходу, який поєднує візуальний аналіз та статистичні методи оцінювання, дозволяє ефективно визначати якість генераторів псевдовипадкових чисел. Найкращі характеристики продемонстрували сучасні генератори, зокрема генератор Mersenne Twister та криптографічні підходи, які забезпечують близькість до теоретичних статистичних параметрів та відсутність кореляційних залежностей. Водночас встановлено, що класичні алгоритми та невдалий вибір параметрів можуть призводити до суттєвого зниження якості генерації, що обмежує можливість їх використання у відповідальних прикладних задачах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження здійснено комплексний порівняльний аналіз генераторів псевдовипадкових послідовностей, зокрема лінійного конгруентного генератора, методу середніх квадратів, генератора Mersenne Twister та генератора на основі криптографічного хешу. Розроблений програмний засіб дозволив поєднати візуальні та статистичні методи оцінювання якості згенерованих послідовностей, що забезпечило більш об’єктивне та наочне дослідження їх властивостей.

На основі отриманих результатів встановлено, що найвищу якість псевдовипадковості демонструють генератор Mersenne Twister та криптографічні генератори, які забезпечують близькість статистичних характеристик до теоретичних значень, рівномірність розподілу та відсутність суттєвих кореляційних залежностей. Лінійний конгруентний генератор може бути придатним для використання за умови правильного вибору параметрів, однак залишається чутливим до їх налаштування, що обмежує його універсальність. Метод середніх квадратів показав найгірші результати через швидке виродження послідовності, що підтверджує його непридатність для практичного застосування.

Проведене дослідження підтверджує, що вибір генератора псевдовипадкових чисел має здійснюватися з урахуванням конкретної сфери застосування, оскільки універсального рішення не існує. Для задач моделювання доцільно використовувати генератори з високими статистичними характеристиками та великим періодом, тоді як у криптографії ключове значення мають непередбачуваність і стійкість до атак.

Перспективи подальших досліджень полягають у розширенні переліку досліджуваних генераторів за рахунок сучасних алгоритмів (зокрема сімейств XORSHIFT та PCG), а також у поглибленому застосуванні стандартизованих тестових наборів, таких як NIST SP 800-22. Доцільним є також дослідження впливу початкової ініціалізації (seed) на якість генерації, аналіз генераторів у багатовимірних задачах та оцінювання їх продуктивності в умовах реальних програмних систем. Окремим напрямом може

стати інтеграція розробленого програмного засобу в навчальні та дослідницькі платформи для підвищення ефективності вивчення та аналізу генераторів псевдовипадкових чисел.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Щербина, Ю., та ін. (2023). Вибір джерела випадковості для комп'ютерного моделювання. *Science-Based Technologies, 59*(3), 233–238. https://doi.org/10.18372/2310-5461.59.17944
2. Костів, Ю. М., Максимович, В. М., Гарасимчук, О. І., Совин, Я. Р., & Мандрона, М. М. (2013). Визначення оптимальних параметрів генератора Голлманна за допомогою статистичних тестів NIST. *Автоматика, вимірювання та керування, 753*, 30–41.
3. Antunes, B. (2025). Statistical quality and reproducibility of pseudorandom number generators in machine learning technologies. *International Journal of Data Informatics and Intelligent Computing, 4*(3), 23–32. https://doi.org/10.59461/ijdiic.v4i3.214
4. Barker, E., & Kelsey, J. (2015). *Recommendation for random number generation using deterministic random bit generators (NIST Special Publication 800-90A Rev. 1).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90Ar1
5. Foreman, C., Yeung, R., & Curchod, F. J. (2024). Statistical testing of random number generators and their improvement using randomness extraction. *Entropy, 26*(12), 1053. https://doi.org/10.3390/e26121053
6. Kovalchuk, L. V., Koriakov, I. V., & Bespalov, O. Y. (2024). Statistical tests for checking independence of random variables, which describe sequences generation in cryptoalgorithms. *Èlektronnoe Modelirovanie, 46*(3), 22–38. https://doi.org/10.15407/emodel.46.03.022
7. L'Ecuyer, P. (2007). Random number generation. In *Handbook of simulation: Principles, methodology, advances, applications, and practice* (pp. 93–137). https://doi.org/10.1002/9780470172445.ch4
8. Marsaglia, G. (2003). Xorshift RNGs. *Journal of Statistical Software, 8*(14). https://doi.org/10.18637/jss.v008.i14
9. Matsumoto, M., & Nishimura, T. (1998). Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS), 8*(1), 3–30. https://doi.org/10.1145/272991.272995
10. O'Neill, M. (2014). *PCG: A family of simple fast space-efficient statistically good algorithms for random number generation*. Harvey Mudd College.
11. Schären, T. M., Hanne, T., & Dornberger, R. (2022). The Xoshiro+ pseudorandom number generator in a computer chess program. In A. Abraham, A. Engelbrecht, F. Scotti, N. Gandhi, P. M. Mishra, G. Fortino, V. Sakalauskas, & S. Pllana (Eds.), *Proceedings of the 13th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2021)* (pp. 33–42). Springer. https://doi.org/10.1007/978-3-030-96302-6_3

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Tetiana O. Hryshanovych
Ph.D.,Associate Professor, Head of the Department of Computer Science and Cybersecurity
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID: 0000-0002-3595-6964
Hryshanovych.Tatiana@vnu.edu.ua

Yana V. Androshchuk
student
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID: 0009-0001-7905-4962
Androshchuk.Yana2023@vnu.edu.ua

Yana S. Yarmolska
student
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID: 0009-0007-0234-8640
Yarmolska.Yana2023@vnu.edu.ua

COMPARATIVE ANALYSIS OF PSEUDORANDOM SEQUENCE GENERATORS AND THEIR EVALUATION

Abstract. The paper investigates the features and performance of pseudorandom sequence generators as essential components of modern information systems used in data processing, simulation, cryptography, and software testing. The study focuses on a comparative analysis of four approaches: the linear congruential generator, the middle-square method, the Mersenne Twister generator, and a generator based on cryptographic hashing. A dedicated software tool was developed to simulate the operation of these generators and to provide their comprehensive evaluation using both statistical and visual analysis techniques. To assess the quality of the generated sequences, the Pearson chi-square test, variance estimation, and autocorrelation analysis were applied. The obtained results are presented in the form of histograms and sequence plots, enabling a clear evaluation of distribution uniformity, randomness, and the presence of hidden patterns in the generated data. The analysis demonstrates that the Mersenne Twister and cryptographic generators exhibit the best statistical properties, including values close to theoretical expectations, minimal autocorrelation, and high uniformity of distribution. It was found that the linear congruent generator can produce acceptable results only with carefully selected parameters, while the middle-square method shows rapid degradation of sequences and poor statistical quality, making it unsuitable for practical applications. The findings confirm the importance of selecting an appropriate generator depending on the application domain and required statistical or cryptographic properties. The proposed comprehensive evaluation approach can be effectively applied in both educational and practical contexts for analyzing and comparing pseudorandom number generators.

Keywords: pseudorandom numbers; generation algorithms; Mersenne Twister generator; linear congruent generator; statistical analysis; autocorrelation; Pearson chi-square test.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shcherbyna, Yu., et al. (2023). Selection of a source of randomness for computer modeling. *Science-Based Technologies, 59*(3), 233–238. https://doi.org/10.18372/2310-5461.59.17944
2. Kostiv, Yu. M., Maksymovych, V. M., Harasymchuk, O. I., Sovyn, Ya. R., & Mandrona, M. M. (2013). Determination of optimal parameters of the Hollmann generator using NIST statistical tests. *Automation, Measurement and Control, 753*, 30–41.
3. Antunes, B. (2025). Statistical quality and reproducibility of pseudorandom number generators in machine learning technologies. *International Journal of Data Informatics and Intelligent Computing, 4*(3), 23–32. https://doi.org/10.59461/ijdiic.v4i3.214
4. Barker, E., & Kelsey, J. (2015). *Recommendation for random number generation using deterministic random bit generators (NIST Special Publication 800-90A Rev. 1).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90Ar1

5. Foreman, C., Yeung, R., & Curchod, F. J. (2024). Statistical testing of random number generators and their improvement using randomness extraction. *Entropy*, *26*(12), 1053. https://doi.org/10.3390/e26121053
6. Kovalchuk, L. V., Koriakov, I. V., & Bespalov, O. Y. (2024). Statistical tests for checking independence of random variables, which describe sequences generation in cryptoalgorithms. *Èlektronnoe Modelirovanie*, *46*(3), 22–38. https://doi.org/10.15407/emodel.46.03.022
7. L'Ecuyer, P. (2007). Random number generation. In *Handbook of simulation: Principles, methodology, advances, applications, and practice* (pp. 93–137). https://doi.org/10.1002/9780470172445.ch4
8. Marsaglia, G. (2003). Xorshift RNGs. *Journal of Statistical Software*, *8*(14). https://doi.org/10.18637/jss.v008.i14
9. Matsumoto, M., & Nishimura, T. (1998). Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, *8*(1), 3–30. https://doi.org/10.1145/272991.272995
10. O'Neill, M. (2014). *PCG: A family of simple fast space-efficient statistically good algorithms for random number generation*. Harvey Mudd College.
11. Schären, T. M., Hanne, T., & Dornberger, R. (2022). The Xoshiro+ pseudorandom number generator in a computer chess program. In A. Abraham, A. Engelbrecht, F. Scotti, N. Gandhi, P. M. Mishrai, G. Fortino, V. Sakalauskas, & S. Pllana (Eds.), *Proceedings of the 13th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2021)* (pp. 33–42). Springer. https://doi.org/10.1007/978-3-030-96302-6_3

Отримано редакцією журналу / Received: 02.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26