УДК 004.9 **DOI: 10.20998/2078-9130.2025.2.346216**

М. В. НЕКРАСОВА

МЕТОДИ ТЕСТУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У статті розглянуто сучасні підходи до оцінювання якості випадкових та псевдовипадкових бітових послідовностей, що використовуються в інформаційних, телекомунікаційних та радіоелектронних системах. Проаналізовано основні вимоги до генераторів випадкових і псевдовипадкових чисел, а також наведено огляд поширених методів перевірки їх статистичних властивостей. Особливу увагу приділено пакетам статистичних тестів, які застосовуються для визначення ступеня наближеності сформованих послідовностей до ідеально випадкового процесу. Розглянуто структуру та принципи роботи стандартного пакета статистичних тестів NIST, що широко використовується для перевірки генераторів псевдовипадкових чисел у задачах криптографії, моделювання та цифрової обробки сигналів. За допомогою системи статистичних тестів NIST проведено дослідження статистичних характеристик послідовностей, сформованих розробленими генераторами псевдовипадкових чисел. Виконано перевірку їх властивостей на випадковість шляхом порівняння отриманих статистичних показників із характеристиками ідеально випадкового ряду. У результаті експериментального аналізу визначено пороговий рівень проходження тестів пакета NIST, який може бути використаний як критерій придатності генератора до практичного застосування. На основі отриманих результатів сформульовано інженерні рекомендації щодо вибору генераторів псевдовипадкових чисел, що демонструють найкращі статистичні характеристики та найбільшу кількість успішно пройдених тестів. Показано, що для стендів напівнатурного моделювання асинхронних радіоелектронних систем доцільним є використання генератора псевдовипадкових чисел, реалізованого на основі методу Мерсенна- Твістера. Крім того, встановлено необхідність подальшого вдосконалення розроблених генераторів шляхом оптимізації їхніх вхідних параметрів та алгоритмічних характеристик з метою підвищення ймовірності успішного проходження статистичних тестів і покращення якості сформованих послідовностей.

Ключові слова: генератори випадкових послідовностей, послідовність біт, псевдовипадкова послідовність, статистичні тести, статистичні тести NIST, випадковість, методи моделювання.

M. NEKRASOVA

METHODS FOR TESTING GENERATORS OF RANDOM AND PSEUDORANDOM SEQUENCES

The article considers modern approaches to evaluating the quality of random and pseudorandom bit sequences used in information, telecommunication, and radio-electronic systems. The main requirements for random and pseudorandom number generators are analyzed, and an overview of commonly used methods for testing their statistical properties is presented. Particular attention is given to statistical test suites applied to determine the degree of similarity between generated sequences and an ideally random process. The structure and operating principles of the NIST statistical test suite, which is widely used for validating pseudorandom number generators in cryptography, modeling, and digital signal processing tasks, are examined. Using the NIST statistical test system, a study of the statistical characteristics of sequences generated by the developed pseudorandom number generators was carried out. Their randomness properties were evaluated by comparing the obtained statistical indicators with those of an ideally random sequence. As a result of the experimental analysis, a threshold level for passing the NIST tests was determined, which can be used as a criterion for assessing the suitability of a generator for practical applications. Based on the obtained results, engineering recommendations were developed for selecting pseudorandom number generators that demonstrate the best statistical characteristics and the largest number of successfully passed tests. It is shown that for hardware-in-the-loop simulation stands of asynchronous radio-electronic systems, it is advisable to use a pseudorandom number generator based on the Mersenne Twister method. In addition, the necessity of further improving the developed generators was established by optimizing their input parameters and algorithmic characteristics in order to increase the probability of successfully passing statistical tests and to improve the quality of the generated sequences.

Keywords: random sequence generators, bit sequence, pseudorandom sequence, statistical tests, NIST statistical tests, randomness, modeling methods.

Вступ. У сучасному світі велике значення мають генератори випадкових та псевдовипадкових послідовностей біт. Вони широко застосовуються у різних задачах: моделюванні, вибіркових методах, чисельному аналізі, програмуванні та криптографії.

Випадкові та псевдовипадкові послідовності грають величезну роль для криптографії – від їхньої якості залежить секретність інформації. Тому завдання створення хороших генераторів та ефективних методів їх оцінки становить великий інтерес [1,2].

Формовані різними способами потоки псевдовипадкових чисел повинні описуватися різними законами розподілу, серед яких найбільш важливими є рівномірний, Гауса, Релея, Райса та експоненціальний. Для формування подібних розподілів використовуються генератори випадкових та псевдовипадкових чисел. Генератори випадкових чисел привабливі з погляду різноманіття їх послідовностей. У той же час, відтворюваність статистичних характеристик генераторів псевдовипадкових чисел (ГПВЧ) робить їх використання для стендів напівнатурного моделювання більш застосовними в порівнянні з генераторами випадкових чисел. Основою для

формування псевдовипадкових чисел з різними законами розподілу є рівноймовірні випадкові числа, які можуть формуватися та перетворюватися на числа з необхідними для моделювання законами розподілу. Необхідність практичного застосування ГПВЧ робить актуальним проведення аналізу чисел, що формуються ними, на випадковість [3].

В якості системи тестування послідовностей чисел на випадковість найбільш широко використовується система тестів NIST, розроблена лабораторією інформаційних технологій Національного інституту стандартів і технологій [4-6]. Тести NIST показують схожість статистичних властивостей сформованого псевдовипадкового ряду чисел із еталонною статистикою ідеально випадкової послідовності.

Мета та постановка задачі. Метою даної роботи є аналіз проходження тестів двійкових послідовностей, формованих генераторами псевдовипадкових чисел, на випадковість з допомогою тестів NIST з урахуванням розроблених програмних засобів моделювання.

Для досягнення поставленої мети необхідне вирішення наступних завдань:

- Проведення аналітичного огляду за методами формування псевдовипадкових послідовностей, розподілених за рівномірним законом;
- Проведення аналітичного огляду по системі статистичних тестів NIST для оцінки послідовностей чисел на випадковість;
- Створення засобів моделювання генераторів псевдовипадкових послідовностей з обраними параметрами та їх оцінка на випадковість;
- Вироблення інженерних рекомендацій щодо вибору генератора псевдовипадкових чисел, що характеризується найбільшою кількістю успішно пройдених тестів.

Методи побудови генераторів випадкових чисел. У звичайному житті випадкові числа можна отримати, підкидаючи монетку або гральні кістки, витягуючи карти з колоди, кулі з урни і т. д. Однак у сучасних комп'ютерних системах використовуються інші методи. Розглянемо наступні існуючі варіанти генераторів:

А) Генератор істинно випадкових послідовностей біт (ГВП). Джерелом випадковості є фізичний процес. Це може бути шум в електронних компонентах, радіоактивний розпад, лічильник фізичних частинок, атмосферний шум, виміряний радіоприймачем тощо [1]. Як правило такі генератори являють собою окремі апаратні модулі для обчислювальної машини, хоча сучасні комп'ютери мають вбудовані апаратні генератори. ГВП найчастіше застосовують у криптографії (ще їх називають криптографічно стійкими генераторами випадкових послідовностей біт - КГВП).

Б) Генератор псевдовипадкових послідовностей чисел (ГПВЧ). У таких генераторах джерелом випадковості є детермінований алгоритм.

Насправді псевдовипадкові послідовності взагалі не є випадковими. Вони обчислюються за допомогою алгоритму з урахуванням деякого початкового числа. І, знаючи початкове число, можна передбачити всі наступні псевдовипадкові числа. Варто відзначити криптографічно стійкі ГПВЧ, які мають жорсткіші вимоги. Криптографічні генератори ПВЧ (КГПВЧ) створюються з використанням функцій потокових шифрів, блокових шифрів, односторонніх функцій та блоків стохастичного перетворення.

В) Комбінований метод застосовується для криптографії. Тут початковий стан генератора береться з ГВП (тобто з фізичного джерела), а потім КГПВЧ формуються випадкові послідовності. До криптографічних генераторів застосовуються особливі вимоги (на відміну від звичайних генераторів): хороші статистичні властивості (сформовані послідовності не повинні відрізнятися від істинно випадкових), великий період послідовності, що формується (відноситься до КГПВЧ). Обчислювально неможливо передбачити попередні значення генератора, маючи фрагмент його показань, генеровані послідовності повинні бути незалежними [2]. В таблиці 1 наведені переваги й недоліки генератору випадкових чисел (ГВЧ) в порівнянні з ГПВЧ [3]]

Таблиця 1 – Переваги та недоліки ГВЧ над ГПВЧ

Переваги	Недоліки
Не періодичний	Повільний
Передбачуваність випадкових чисел не заснована на знаннях попередніх значень	Громіздкий для встановлення та запуску
Не існує жодних залежностей	Випадкові послідовності не відтворювані
Високий рівень безпеки	Дороговартісний
Не заснований на алгоритмах	Можливість впливу на покази

Алгоритми побудови псевдовипадкових чисел. Для формування псевдовипадкових чисел із рівномірним розподілом на стенді напівнатурного моделювання широко використовуються методи на основі М-послідовностей. Такі генератори будуються з використанням зсувних регістрів, що обираються з початкових умов.

Метод М-послідовності формує ряд двійкових чисел відповідно до рекурентної формули:

$$x_{n+p}=c_{p-1}\cdot x_{n+p-1}+ c_{p-2}\cdot x_{n+p-2}+\ldots+c_1\cdot x_{n+1}+x_n(mod\ 2), \quad (1)$$

$n=1,2,3,\ldots,$

де $c_1, c_2, c_3, \ldots, c_{p-1}$ - коефіцієнти зворотного зв'язку, визначені за допомогою породжувального поліному, p – параметр зсуву.

М-послідовність характеризується такими властивостями:

- є періодичною з періодом $N=2^n-1$, де n – довжина регістру, за допомогою якого формується М-послідовність;
- розподіл символів у періоді є рівноймовірним;
- М-послідовність містить усі n-значні комбінації двійкових символів, крім нульової комбінації.

У зв'язку з вивченістю та відносною простотою методу М-послідовності сформований масив псевдовипадкових чисел має легко виявні статистичні закономірності та недостатній рівень випадковості.

У роботі [7-9] запропоновано ГПВЧ, побудований на зсувних регістрах за умов формування циклів немаксимальної довжини, який дає змогу створювати набори псевдовипадкових чисел із різноманітними ймовірносними та кореляційними властивостями. Також відомий генератор гіперхаотичних сигналів [9-12], побудований на основі хаотичних систем і такий, що формує псевдовипадкові сигнали, які можна використовувати для забезпечення прихованості та надійності передавання даних.

У цій роботі розглядаються програмні засоби моделювання генераторів, що формують псевдовипадкові послідовності, побудовані на основі п'ятипараметричного методу, методу Таусворта, комбінованого методу Таусворта та методу Мерсенна Твістера.

П'ятипараметричний метод будується на основі зсувного регістра зі зворотним зв'язком і використовує характеристичний поліном із п'яти членів, що дає змогу генерувати послідовності w-бітових двійкових цілих чисел відповідно до рекурентної формули:

$$X_{n+p}= X_{n+q1}+ X_{n+q2}+ X_{n+q3}+ X_n(mod2),\ n=1,2,3,\ldots \quad (2)$$

де X_n - черговий біт послідовності, p, q - параметри зсуву (ступені характеристичного полінома),

Під час реалізації генератора на основі п'ятипараметричного методу були обрані такі параметри: $p = 89$; $q_1 = 20$; $q_2 = 40$; $q_3 = 69$; $w = 64$ (кількість біт, довжина слова).

Генератор псевдовипадкових чисел на основі методу Таусворта використовує рекурентну формулу:

$$X_n= X_{nt}, X_{nt+1}, \ldots, X_{nt+w-1}, X_{n+p}= X_{n+q}+ X_n\ (mod2), \quad (3)$$
$$n=0,1,2,\ldots$$

Обрані параметри генератора на основі методу Таусворта: $p = 16$; $q = 7$; w = 16; t = 19 (зсув при формуванні виходу).

Комбінований метод Таусворта являє собою комбінацію кількох простих послідовностей Таусворта з однаковою довжиною слова w і визначається формулою:

$$X_n= X_n^{(1)}+ X_n^{(2)}+\ldots+ X_n^{(J)} mod(2),\ n=0,1,2,\ldots \quad (4)$$

Генератор на основі комбінованого методу Таусворта розроблявся за допомогою трьох простих послідовностей з параметрами: $p = 16$; $w = 16$; $t = 19$.

Метод Мерсенна Твістера дозволяє генерувати послідовність двійкових псевдовипадкових w-бітових чисел за рекурентною формулою:

$$X_{n+p}= X_{n+q}+ (X_n|\ X_{n+1})^{(r)}A(mod2),\ n=1,2,3,\ldots, \quad (5)$$

де $(X_n|\ X_{n+1})^{(r)}$ – двійкове число, що отримане шляхом конкатенації чисел X_n і X_{n+1} , коли перші $(w- r)$ біт взяли з X_n , останні r біт – з X_{n+1}; A - матриця, що складається з нулів і одиниць та визначена за допомогою певного числа a.

Для покращення рандомізації отриманого ряду застосовується метод загартування, який визначається за такими формулами:

$$\begin{aligned} y1_n &= X_{n+p};\\ y2_n&=(y1_n+(y1_n>>u));\\ y3_n&= (y2_n+(y2_n<<s)\cdot b);\\ y4_n&= (y3_n+(y3_n<<t)\cdot c);\\ y5_n&=(y4_n+(y4_n>>l));\\ y_n&= y5_n. \end{aligned} \quad (6)$$

Для реалізації генератора на основі методу Мерсенна Твістера обрані наступні параметри: $p = 624$; $q = 397$; $w = 32$; $r = 31$; $u = 11$; $s = 7$; $t = 15$; $l = 18$.

Дослідження ГПВЧ. Для дослідження розроблених генераторів на випадковість оцінювалися результати проходження псевдовипадковими послідовностями 15 тестів NIST [7, 13-15], наведених у табл. 2.

Система тестів побудована на основі перевірки нульової гіпотези. Нульовою гіпотезою приймається припущення, що перевірювана двійкова послідовність є істинно випадковою. У цьому випадку послідовність матиме хороші статистичні характеристики. Альтернативною гіпотезою вважається припущення про те, що тестована послідовність не є випадковою.

На вхід кожного тесту подавалися сформовані генераторами псевдовипадкових чисел кінцеві послідовності, для яких обчислювалася статистика, що характеризує певну їх властивість. Для оцінки послідовностей на випадковість отримана статистика порівнювалася з еталонною статистикою випадкового ряду. За результатами порівняння обчислювалося значення P, що характеризує схожість послідовності, сформованої розробленим генератором, з ідеально випадковою послідовністю. Отримане значення P порівнювалося з рівнем значущості α, $\alpha \in [0{,}001; 0{,}01]$.

За допомогою пакету MATLAB розроблено модель формування псевдовипадкових послідовностей та перевірки сформованої послідовності на випадковість за допомогою тестів NIST шляхом обчислення ймовірності проходження тестів при проведенні 10 000 дослідів.

Таблця 2 – Опис тестів NIST

	Назва тесту	***Дефект, що визначається***
1	Частотний побітовий тест	Визначає співвідношення одиниць і нулів у послідовності
2	Частотний блоковий тест	Визначає співвідношення одиниць і нулів у блоці визначеної довжини
3	Тест на послідовність однакових бітів	Визначає ступінь чергування одиниць і нулів у послідовності
4	Тест на найдовшу послідовність одиниць у блоці	Визначає співвідношення між найдовшим рядом одиниць у блоці та очікуваною довжиною ряду одиниць у випадковій послідовності
5	Тест рангу бінарних матриць	Виконує обчислення рангів неперетинних підматриць, утворених початковою двійковою послідовністю
6	Спектральний тест	Оцінює висоти піків під час дискретного перетворення Фур'є початкової послідовності
7	Тест приблизної ентропії	Оцінює частоту всіх можливих перекривань блоків визначеної довжини
8	Тест на збіг неперетинних шаблонів	Оцінює кількість наперед визначених шаблонів у початковій послідовності
9	Тест на збіг перетинних шаблонів	Оцінює кількість шаблонів, утворених початковою послідовністю зі зсувом на 1 біт
10	Тест на підпослідовності	Оцінює частоту знаходження всіх можливих послідовностей визначеної довжини всередині початкової послідовності
11	Тест на довільні відхилення	Виконує обчислення кумулятивних сум для 8 станів циклів, утворених за допомогою початкової послідовності
12	Різновид тесту на довільні відхилення	Виконує обчислення кумулятивних сум для більшої кількості станів циклів порівняно з попереднім тестом.
13	Тест на лінійну складність	Аналізує початкову послідовність за принципом роботи лінійного зсувного регістра зі зворотним зв'язком
14	Тест кумулятивних сум	Виконує обчислення кумулятивних сум початкової послідовності від першого елемента до останнього та від останнього до першого відповідно
15	Універсальний статистичний тест Маурера	Оцінює ступінь стиснення початкової послідовності

Під час запуску моделі змінна i, що визначає порядковий номер перевірюваного генератора псевдовипадкових чисел, встановлюється рівною 1. Для обраного генератора визначаються заздалегідь задані вхідні параметри та формується двійкова псевдовипадкова послідовність довжиною 1 000 000 біт. Сформована послідовність одночасно проходить 15 тестів NIST. За результатами 100 000 дослідів накопичується статистика, під час якої оцінюється ймовірність проходження тестів для 1-го генератора. Аналогічний принцип розрахунку ймовірності застосовується для інших генераторів псевдовипадкових чисел (при $i = 2…5$).

Результати моделювання і тестування та їх обговорення. Розроблено програмні засоби моделювання для дослідження двійкових послідовностей на «випадковість» за допомогою тестів NIST. Оцінка проводилася за ймовірністю проходження тестів двійковими послідовностями довжиною 1 000 000 біт, сформованими генераторами псевдовипадкових чисел на основі методу М-послідовності (Ген. № 1), п'ятипараметричного методу (Ген. № 2), методу Таусворта (Ген. № 3), комбінованого методу Таусворта (Ген. № 4), методу Мерсенна Твістера (Ген. № 5). Отримані ймовірності проходження тестів NIST генераторами при проведенні 10 000 дослідів наведені в табл. 3.

Для спрощення аналізу отриманих результатів успішність проходження тесту відповідного генератора оцінювалася за рівнем порогової ймовірності, що дорівнює 0,7. Кількість успішно пройдених тестів NIST для розроблених генераторів псевдовипадкових чисел наведена на рис. 1.

Таблиця 3 – Оцінки ймовірностей проходження тестів NIST

	Тест 1	Тест 2	Тест 3	Тест 4	Тест 5	Тест 6	Тест 7	Тест 8
Ген.№1	0,9997	0,9997	0,9997	0,9691	0	0	0,9997	0,0306
Ген.№2	0,3194	0	0,1575	0	0,9927	0	0,0012	0
Ген.№3	0,9773	0,9734	0,9816	0	0	0	0,9999	0,9847
Ген.№4	0,4798	0,8132	0,3530	0,3127	0,9429	0,0006	0,0770	0,8526
Ген.№5	0,9898	0,9890	0,9889	0,5687	0,9921	1	0,9999	0,9894
	Тест 9	Тест 10	Тест 11	Тест 12	Тест 13	Тест 14	Тест 15	
Ген.№1	0,9997	0,9997	0,0014	0,5278	0	0,9997	0,9997	
Ген.№2	1	0,0135	0,4048	0,9029	0,9895	0,0171	1	
Ген.№3	0,9999	0,9951	0,0469	0,8553	0	0,9806	0,9999	
Ген.№4	0,9715	0,1091	0,2843	0,8947	0,9537	0,4974	0,9878	
Ген.№5	1	0,9821	0,0807	0,7022	0,9901	0,9903	1	

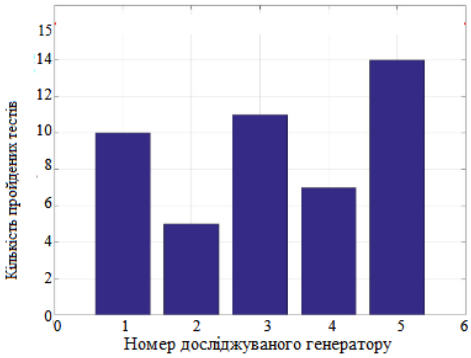

Рис. 1 – Кількість тестів, що пройшли генератори

Найменша кількість пройдених тестів характерна для генераторів № 2 і № 4. Генератори № 1 і № 3 мають порівнянну кількість пройдених тестів. Найбільш наближеною до еталонного випадкового ряду є послідовність, сформована генератором на основі методу Мерсенна Твістера (Ген. № 5), яка характеризується найбільшою кількістю успішно пройдених тестів NIST – 14.

Подальший аналіз табл. 3 показує, що існують нульові ймовірності проходження тестів генератором № 1 для тестів № 5, № 6, № 13; генератором № 2 — для тестів № 2, № 4, № 6, № 8; генератором № 3 — для тестів № 4, № 5, № 6, № 13 при обраних параметрах моделювання.

Встановлено, що підвищення ймовірності проходження деяких тестів можливо досягти варіацією вхідних параметрів методу генерації, що формує послідовність із вищим рівнем «випадковості». Для розробки оптимальних з точки зору «випадковості» вхідних параметрів розроблених генераторів потрібні додаткові дослідження, які виходять за рамки даної роботи.

Слід також зазначити низьку ймовірність проходження тестів № 4, № 6, № 11 послідовностями, сформованими генераторами при обраних параметрах. Низька ймовірність проходження тесту № 4 свідчить про появу довгих послідовностей одиниць (нолів). Низька ймовірність проходження тесту № 6 показує наявність великої кількості спектральних піків у перевірюваних послідовностях, що підтверджується рис. 2, на якому наведена спектральна характеристика генератора, побудованого на основі М-послідовності. Для порівняння на рис. 2 наведено пороговий рівень, відносно якого очевидна наявність у спектрі перевірюваного сигналу високих піків.

Результати тесту № 11 показують наявність великої величини відхилень при обчисленні кумулятивних сум восьми станів послідовностей; однак у цьому тесті можливі неоднозначності результатів проходження, і в такому випадку рішення про схожість перевірюваної послідовності з ідеально випадковою приймається на основі інших тестів.

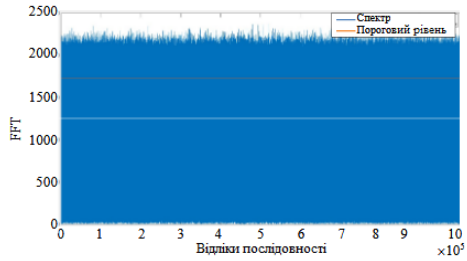

Рис. 2 – Спектральна характеристика послідовності

Висновок. У цій статті розроблено засоби моделювання генераторів псевдовипадкових чисел та проведено перевірку сформованих ними послідовностей на випадковість шляхом проходження тестів NIST.

Проведений аналіз проходження тестів NIST показав, що псевдовипадкові послідовності, сформовані методами М-послідовності - відповідають 10 тестам, п'ятипараметричним методом - 5 тестам, методом Таусворта - 11 тестам, комбінованим методом Таусворта - 7 тестам, методом Мерсенна Твістера - 14 тестам з ймовірністю не менше 0,7.

За результатами оцінки встановлено, що як генератори псевдовипадкових чисел для стендів напівнатурного моделювання асинхронних радіоелектронних систем рекомендується застосовувати метод Мерсенна Твістера.

Крім того, оцінки ймовірностей проходження тестів послідовностями, розглянутими в даній роботі, свідчать про необхідність подальшого вдосконалення генераторів псевдовипадкових чисел з метою підвищення ймовірності їх проходження статистичних тестів.

Список літератури

1. Random Number Generators: An Evaluation and Comparison of Random.org and SomeCommonly Used Generators (2005). Режим доступу: https://www.random.org/analysis/Analysis2005.pdf
2. Security Requirements For Cryptographic Modules (2001). Режим доступу:http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
3. Brown R. Dieharder: A Random Number Test Suite (2024). Режим доступа:http://www.phy.duke.edu/~rgb/General/dieharder.php
4. Rukhin A., Soto J., Nechvatal J. et al (2010). A statistical test suite for random and pseudorandom number generators for cryptographic application / // NIST Special Publication. 800-22 Revision la. Gaithersburgational Institute of Standards and Technology, 131 p.
5. Recommendation for the Entropy Sources Used for Random Bit Generation (2016). Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
6. Recommendation for Random Bit Generator (RBG) Constructions (2012). Режим доступу:http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf
7. Maksymovych, V., Shevchuk, M., & Mandrona, M. (2016). *Research of pseudorandom bit sequence generators based on LFSR*. Lviv Polytechnic National University. *https://ena.lpnu.ua/items/215c5cc2-816a-4a46-89db-259eb7ae3be3*
8. Poluyanenko, N. (2017). *Development of the search method for nonlinear shift registers using hardware, implemented on field programmable gate arrays*. European Journal of Engineering, 5(3), 45–53. https://journal.eu-jr.eu/engineering/article/view/271 https://doi.org/10.21303/2461-4262.2017.00271
9. Zhang, X.-F., & Fan, J.-L. (2010). *Pseudo-random sequence generating method based on LFSR and chaotic system*. Acta Physica Sinica, 59(3), 2289–2295. https://wulixb.iphy.ac.cn/en/article/doi/10.7498/aps.59.2289 https://doi.org/10.7498/aps.59.2289
10. Muhhamad, I. et al. (2020). *Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM)*. Electronics, 9(1), 104. https://www.mdpi.com/2079-9292/9/1/104 https://doi.org/10.3390/electronics9010104
11. Nguyen, N. T., & Bui, T. Q., et al. (2021). *Designing a pseudo-random bit generator with a novel 5D-hyperchaotic system*. arXiv. https://arxiv.org/abs/2105.08896
12. Kushnir, M. Ya., Kosovan, H. V., & Kroyalo, P. M. (2022). *Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems*. Research in Cybernetics, 18(2), 112–125. https://ric.zp.edu.ua/article/view/254427
13. Кузьменко О. В., Ткаченко В. А. Методи оцінки якості та криптостійкості випадкових послідовностей // Захист інформації. 2023. Т. 25, № 2. С. 45–53.
14. Іванченко І. С. Методи тестування псевдовипадкових послідовностей // Інформаційні технології та моделювання. 2022. № 1. С. 78–85.
15. Петренко О. М. Аналіз статистичних тестів випадковості для генераторів чисел // Системи обробки інформації. 2021. № 3. С. 112–118.

References (transliterated)

1. Random Number Generators: An Evaluation and Comparison of Random.org and SomeCommonly Used Generators (2005). Режим доступу: https://www.random.org/analysis/Analysis2005.pdf
2. Security Requirements For Cryptographic Modules (2001). Режим доступу: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.*pdf*
3. Brown R. Dieharder: A Random Number Test Suite (2024). Режим доступа:http://www.phy.duke.edu/~rgb/General/dieharder.php
4. Rukhin A., Soto J., Nechvatal J. et al (2010). A statistical test suite for random and pseudorandom number generators for cryptographic application / // NIST Special Publication. 800-22 Revision la. Gaithersburgational Institute of Standards and Technology, 131 p.
5. Recommendation for the Entropy Sources Used for Random Bit Generation (2016). Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
6. Recommendation for Random Bit Generator (RBG) Constructions (2012). Режим доступу: http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf
7. Maksymovych, V., Shevchuk, M., & Mandrona, M. (2016). *Research of pseudorandom bit sequence generators based on LFSR*. Lviv Polytechnic National University. https://ena.lpnu.ua/items/215c5cc2-816a-4a46-89db-259eb7ae3be3
8. Poluyanenko, N. (2017). *Development of the search method for nonlinear shift registers using hardware, implemented on field programmable gate arrays*. European Journal of Engineering, 5(3), 45–53. https://journal.eu-jr.eu/engineering/article/view/271 https://doi.org/10.21303/2461-4262.2017.00271
9. Zhang, X.-F., & Fan, J.-L. (2010). *Pseudo-random sequence generating method based on LFSR and chaotic system*. Acta Physica Sinica, 59(3), 2289–2295. https://wulixb.iphy.ac.cn/en/article/doi/10.7498/aps.59.2289 https://doi.org/10.7498/aps.59.2289
10. Muhhamad, I. et al. (2020). *Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM)*. Electronics, 9(1), 104. https://www.mdpi.com/2079-9292/9/1/104 https://doi.org/10.3390/electronics9010104
11. Nguyen, N. T., & Bui, T. Q., et al. (2021). *Designing a pseudo-random bit generator with a novel 5D-hyperchaotic system*. arXiv. https://arxiv.org/abs/2105.08896
12. Kushnir, M. Ya., Kosovan, H. V., & Kroyalo, P. M. (2022). *Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems*. Research in Cybernetics, 18(2), 112–125. https://ric.zp.edu.ua/article/view/254427
13. Kuzmenko O. V., Tkachenko V. A. Metody otsinky yakosti ta kryptostiikosti vypadkovykh poslidovnostei // Zakhyst informatsii. 2023. Vol. 25, No. 2. P. 45–53.
14. Ivanchenko I. S. Metody testuvannia psevdovypadkovykh poslidovnostei // Informatsiini tekhnolohii ta modeliuvannia. 2022. No. 1. P. 78–85.
15. Petrenko O. M. Analiz statystychnykh testiv vypadkovosti dlia heneratoriv chysel // Systemy obrobky informatsii. 2021. No. 3. P. 112–118.

Надійшла (received) 10.12.2025
Прийнята до друку (accepted) 22.12.2025
Опублікована (published) 29.12.2025

Відомості про авторів/ About the Authors

Некрасова Марія Володимирівна (Nekrasova Mariia) – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри комп'ютерного моделювання процесів та систем; м. Харків, Україна; тел.: (057)-707-64-54; ORCID: https://orcid.org/0009-0006-9285-0740; e-mail: masha12dec@gmail.com