DOI: 10.58254/viti.8.2025.08.104

УДК 004.421.2

д-р. техн. наук, професор Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ ім. Героїв Крут)
Тлустий А. О. ORCID: 0000-0002-4777-9563 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЗАСТОСУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Псевдовипадкові послідовності відіграють ключову роль у сучасних інформаційно-комунікаційних та обчислювальних системах. Напрямки наукових досліджень питань створення та обробки псевдовипадкових послідовностей є невід'ємною складовою розвитку озброєння та військової техніки оскільки у в цій сфері псевдовипадкові послідовності використовуються для забезпечення захищених каналів зв'язку, прихованої передачі інформації, формування завадостійких сигналів, а також у системах радіолокації та навігації. Застосування таких послідовностей дозволяє підвищити точність та стійкість до впливу засобів радіоелектронної боротьби. Особливої ваги набуває проблема генерації якісних псевдовипадкових послідовностей набуває в умовах сучасних бойових дій. Інформаційна перевага та стійкість систем зв'язку до перехоплення чи глушіння визначають ефективність управління військами і застосування окремих високотехнологічних зразків озброєння.

Використання псевдовипадкових послідовностей у технологіях розширеного спектра забезпечує не лише підвищену завадостійкість радіоканалів, але й ускладнює виявлення та дешифрування сигналів з боку противника. Це має безпосереднє значення також для безпілотних авіаційних комплексів, навігаційних систем та високоточних засобів ураження. Крім того, псевдовипадкові послідовності є основою для криптографічних алгоритмів, що забезпечують захист службової інформації, командно-штабних даних та телеметрії озброєння.

Генератори псевдовипадкових послідовностей знаходять застосування в автоматизованих системах управління військами, інформаційних мережах та спеціалізованому програмному забезпеченні військового призначення.

Таким чином, з огляду на тенденції цифровізації та інтелектуалізації озброєння, вимоги до швидкодії, статистичної якості та криптографічної стійкості псевдовипадкових послідовностей, дослідження середовища використання псевдовипадкових послідовностей є актуальним завданням, що напряму пов'язане з підвищенням ефективності функціонування сучасних і перспективних зразків озброєння та військової техніки, а також із забезпеченням інформаційної та кібернетичної безпеки у воєнній сфері.

Ключові слова: *генератор псевдовипадкових послідовностей, криптозахист, статистичні тести, генерація ключів, інформаційно-комунікаційні системи.*

V. Kuzavkov, A. Tlustyi. Analysis of the application of pseudorandom sequences in weapon systems

Pseudorandom sequences play a key role in modern information-communication and computational systems. Research directions devoted to the generation and processing of pseudorandom sequences are an integral component of the development of weaponry and military equipment, since in this domain pseudorandom sequences are employed to provide secure communication channels, covert information transfer, formation of interference-resistant signals, as well as in radar and navigation systems. The use of such sequences makes it possible to increase accuracy and robustness against the effects of electronic warfare means. This problem of generating high-quality pseudorandom sequences acquires particular importance in the conditions of contemporary armed conflict. The information advantage and the resilience of communication systems to interception or jamming determine the effectiveness of troop command and the employment of certain high-technology weapon systems.

Application of pseudorandom sequences in spread-spectrum technologies provides not only enhanced interference resistance of radio channels, but also complicates detection and decryption of signals by the adversary. This is directly relevant for unmanned aerial systems, navigation systems, and precision strike means. Moreover, pseudorandom sequences form the basis of cryptographic algorithms that protect operational information, command-and-control data, and telemetry of weapon systems.

Pseudorandom sequence generators are used in automated command-and-control systems, information networks, and specialized military software solutions.

Thus, in view of trends toward digitization and increased autonomy of weapon systems, and given the stringent requirements for throughput, statistical quality, and cryptographic strength of pseudorandom sequences, investigation of the operating environment and generation methods for pseudorandom sequences is an urgent task directly related to improving the performance of current and prospective weapon systems, as well as to ensuring information and cyber security in the military domain.

Keywords: *pseudorandom sequence generator, cryptographic protection, statistical tests, key generation, information-communication systems.*

Постановка проблеми

Проблематика генерації та застосування псевдовипадкових послідовностей (ПВП) тривалий час перебуває у фокусі наукових досліджень, що обумовлено їх ключовою роллю в інформаційній безпеці та цифрових комунікаційних технологіях. Попри значний науковий прогрес, відсутня систематизована оцінка ролі та ефективності ПВП у військових системах, де вони використовуються для захищеного зв’язку, радіолокації, навігації, формування завадостійких сигналів і криптографічного захисту даних. Наявні дослідження зосереджені переважно на окремих аспектах – статистичній якості, криптографічній стійкості чи апаратних реалізаціях генераторів, тоді як інтегральний підхід до аналізу сфер застосування ПВП у комплексних зразках озброєння відсутній. Це зумовлює необхідність цілісного вивчення можливостей та обмежень ПВП у воєнно-технічних системах для підвищення їхньої ефективності та інформаційної безпеки.

Аналіз публікацій за темою дослідження

У працях українських дослідників [1; 3] наголошується на важливості ПВП для систем військового зв’язку, де основна увага приділяється забезпеченню завадостійкості та захисту службової інформації. Ці підходи корелюють із закордонними дослідженнями [2; 4], у яких ПВП розглядаються як базис для побудови систем зв’язку з розширеним спектром, що гарантують прихованість передавання та стійкість до впливу радіоелектронних засобів противника.

Особливе місце у науковій літературі займають дослідження, спрямовані на створення генераторів криптографічно стійких ПВП. Рекомендації NIST [5; 9] визначають сучасні вимоги до генераторів випадкових чисел, підкреслюючи необхідність як високих статистичних характеристик, так і захисту від можливих криптоаналітичних атак. Значний внесок у цій сфері зробили роботи, що аналізують математичні властивості послідовностей: періодичність, рівномірність розподілу, кореляційні характеристики та лінійну складність [6; 7; 14; 15].

Паралельно активно досліджуються апаратні методи генерації випадкових чисел, які базуються на фізичних процесах, зокрема на хаотичних коливаннях та шумових сигналах [8; 10; 19]. Такі підходи дозволяють отримати справді випадкові послідовності, однак їх впровадження вимагає значних обчислювальних і технічних ресурсів.

Окремий напрям становлять роботи, присвячені застосуванню ПВП у криптографії. Дослідження [24–26] висвітлюють використання генераторів псевдовипадкових чисел у протоколах автентифікації, цифрових підписах, алгоритмах формування ключів та протоколах післяквантової криптографії. Це дозволяє зробити висновок, що саме криптографія є сферою, де до ПВП висуваються найжорсткіші вимоги.

Метою статті є систематизація та обґрунтування сфер застосування ПВП у інформаційно-комунікаційних системах спеціального призначення, визначення їх ролі у забезпеченні криптографічної стійкості та функціональної ефективності технологій передачі, обробки й захисту даних

Виклад основного матеріалу

Визначення та класифікація псевдовипадкових послідовностей

Псевдовипадкові послідовності (ПВП) визначаються як послідовності чисел або бітів, що генеруються детермінованими алгоритмами, але за своїми статистичними властивостями наближаються до істинно випадкових [6].

Класифікація ПВП формують базис для їх подальшого дослідження і дає змогу встановити відповідність певного виду послідовності конкретним сферам застосування у військовій та цивільній техніці. Класифікація ПВП може здійснюватися за різними ознаками (табл. 1).

Таблиця 1

Класифікація ПВП

№ з/п	Критерій класифікації	Класи (Типи) ПВП
1	За призначенням та сферою застосування	Звичайні ПВП Криптографічно стійкі ПВП Сигнальні ПВП (PN-послідовності)
2	За методом генерації	Лінійні генератори Нелінійні генератори Гібридні генератори
3	За структурою та довжиною періоду	Короткоперіодичні Довгоперіодичні
4	За якістю випадковості	Нестійкі ПВП Високоякісні ПВП
5	За способом реалізації	Детерміновані (алгоритмічні) Апаратні
6	У контексті застосувань	Криптографічно стійкі Некриптографічні
7	За структурою генератора	Лінійні конгруентні РЗЛЗЗ -послідовності Хаотичні відображення, гібридні методи

Класифікація псевдовипадкових послідовностей

У науковій та технічній літературі ПВП класифікують за кількома критеріями:

За призначенням та сферою застосування: звичайні ПВП – *застосовуються у моделюванні, чисельних методах, статистиці, машинному навчанні,* криптографічно стійкі ПВП – *розроблені для задач захисту інформації, генерації ключів, формування стійких до атак потоків даних* [8], синальні ПВП (PN-послідовності) – *застосовуються у системах зв’язку, радіолокації та навігації для розширення спектра сигналу та підвищення завадостійкості* [9].

За методом генерації: лінійні генератори *(лінійні конгруентні, регістри зсуву з лінійним зворотним зв’язком)* нелінійні генератори *(алгоритми на основі хаотичних відображень, криптографічних примітивів),* гібридні генератори *(поєднання кількох методів для підвищення статистичної якості).*

За структурою та довжиною періоду: короткоперіодичні – *придатні для обмежених завдань (наприклад, тестових симуляцій),* довгоперіодичні – *забезпечують стійкість до передбачення та можливість використання у складних системах (наприклад, військових мережах зв’язку).*

За якістю випадковості: нестійкі ПВП – *мають виявлені кореляції, що робить їх непридатними для криптографії,* високоякісні ПВП – *проходять усі тести NIST та відповідають вимогам до генераторів випадкових чисел у безпечних системах* [7].

ПВП також поділяють на детерміновані (алгоритмічні), які формуються за допомогою математичних виразів або рекурентних співвідношень, та апаратні, що базуються на фізичних процесах, котрі моделюють випадковість [8].

У контексті криптографії та військових застосувань важливим є поділ ПВП на криптографічно стійкі та некриптографічні. Перші володіють високим рівнем непередбачуваності та захищеності від атак, другі ж використовуються у задачах моделювання чи тестування, де вимоги до безпеки є нижчими [9].

Також ПВП класифікують за структурою генератора: на основі лінійних конгруентних методів, регістрів зсуву з лінійним зворотним зв’язком (РЗЛЗЗ), хаотичних відображень, гібридних методів тощо [10].

Класифікація ПВП демонструє широкий спектр можливостей застосування ПВП. Вибір конкретного класу залежить від вимог до системи: у моделюванні та чисельних обчисленнях

першочерговим є швидкодія, тоді як у військових системах зв’язку та криптографії – криптостійкість і захищеність від передбачення. Саме ця різноманітність підходів до класифікації дозволяє адаптувати ПВП до потреб різних галузей, включаючи сферу озброєнь і військової техніки.

Ключові математичні властивості

Ефективність псевдовипадкових послідовностей (ефективність використання ПВП), зокрема у військовій техніці та засобах зв’язку, безпосередньо залежить від їхніх математичних властивостей. Саме вони визначають, наскільки послідовність наближена до істинно випадкової та чи може вона бути використана для криптографічного захисту, моделювання або формування сигнальних структур. До таких властивостей слід віднести: періодичність; рівномірність розподілу; незалежність (відсутність кореляцій); автокореляційні властивості; лінійна складність; ентропія та непередбачуваність; стійкість до статистичного аналізу. Розглянемо ці показники окремо.

Будь-який детермінований генератор ПВП породжує послідовність скінченої довжини, яка з часом повторюється. Довжина циклу називається періодом. Для практичних застосувань необхідно, щоб період був достатньо довгим і перевищував потреби системи. У криптографії вимагаються надзвичайно довгі періоди [11].

Іншою фундаментальною вимогою до ПВП є рівномірність розподілу значень у заданому діапазоні. Це означає, що з імовірністю, наближеною до випадкової, усі можливі стани генератора повинні зустрічатися з однаковою частотою. У випадку бітових послідовностей – кількість нулів і одиниць має бути збалансованою [12].

Для того щоб ПВП були корисними в задачах захисту інформації та передачі сигналів, вони повинні задовольняти вимогу статистичної незалежності: жоден елемент послідовності не повинен передбачатися на основі попередніх. Наявність кореляцій робить послідовність вразливою до аналізу та атак, що є критичною загрозою у військових системах зв’язку [13].

У багатьох прикладних сферах, зокрема у радіолокації та навігації, важливою є форма автокореляційної функції ПВП (рис. 1). Ідеальна послідовність повинна мати низькі бічні пелюстки автокореляції та різке зростання у точці нульового зсуву. Такі властивості забезпечують чітке розрізнення сигналів і зменшують рівень перешкод [14].

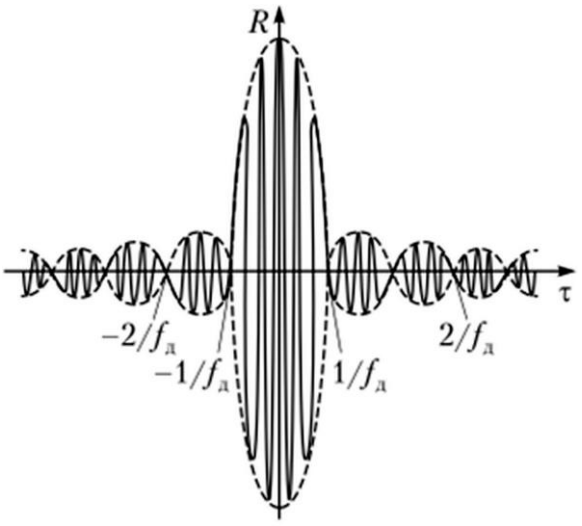

Рис. 1. Графік нормованої автокореляційної функції лінійно-частотно модульованого імпульсу

Лінійна складність визначається як мінімальна довжина регістра зсуву, здатного відтворити дану послідовність. Для безпечних ПВП лінійна складність повинна бути високою, інакше існує ймовірність відтворення генератора та передбачення подальших значень [15].

Ентропія визначає ступінь «невпорядкованості» послідовності та гарантує, що прогнозування наступного елемента практично неможливе. Висока ентропія є необхідною умовою для використання ПВП у криптографії. У військових застосуваннях ця властивість безпосередньо пов'язана з кіберстійкістю та захистом від засобів радіоелектронної розвідки [13].

Придатність визначається за допомогою статистичних тестів. Цей набір найчастіше визначається сукупністю нормативних документів та стандартів, серед яких ключовими є NIST SP 800-22, NIST SP 800-90, ISO/IEC 18031, FIPS 140-2/3, а також національні стандарти (ДСТУ ISO/IEC 18031:2015). Це дозволяє визначити, чи відповідають їхні властивості вимогам реальних систем. Послідовності, що не проходять таких тестів не можуть застосовуватися у критичних задачах [15].

Таким чином, сукупність ключових математичних властивостей ПВП формує основу для їхньої придатності до різних сфер використання. У військових системах особливе значення мають довгий період, рівномірність розподілу, висока лінійна складність та низька кореляція, що дозволяє забезпечувати прихованість, завадостійкість та криптографічну стійкість.

Наступним аспектом роботи є розгляд основних методів генерації ПВП.

Методи генерації псевдовипадкових послідовностей (ПВП) визначають їхню якість, довжину періоду та придатність для різних застосувань. У загальному випадку генератор описується рекурентним співвідношенням:

$$X_{n+1} = f\left(X_{n,}X_{n-1,\dots}X_{n-k+1}\right), \tag{1}$$

де f – функція переходу;

k – порядок генератора [6].

У науковій літературі розрізняють: лінійні методи, не лінійні, гібридні та апаратні.

Реалізація лінійних методів можлива на основі лінійних конгруентних генераторів та РЗЛЗЗ.

При застосуванні лінійних конгруентних генераторів виконується правило:

$$X_{n+1} = (aX_n + c)\mathrm{mod}\, m, \tag{2}$$

де a – множник (ціле число, зазвичай > 1);

c – приростання (ціле число, може бути 0);

X_{n+1} – поточне значення послідовності (ціле число);

m – модуль (ціле число, зазвичай > 0);

$\mathrm{mod}\, m$ – операція взяття залишку від ділення на m.

Вираз (2) є класичним прикладом лінійного конгруенційного генератора, який використовується для створення псевдовипадкових послідовностей.

При правильному виборі параметрів забезпечується максимальний період m [16].

Формула визначає наступне значення послідовності X_{n+1} як залишок від ділення суми $aX_n + c$ на m.

Наприклад:

якщо $X_n = 5$, $a - 3$, $c = 7$, $m - 10$, то $X_{n+1} = (3 \cdot 5 + 7)\mathrm{mod}10 = 22,\ \mathrm{mod}10 = 2.$

У випадку використання РЗЛЗЗ правило виглядає наступним чином:

$$S_{n+k} = (C_1 S_{n+k-1} \oplus C_2 S_{n+k-2} \oplus \dots \oplus C_k S_n, \tag{3}$$

де $\oplus$ – операція XOR, $Ci \in \{0,1\}$ – коефіцієнти з характеристичного многочлена. (ЛЗРЗЗ) утворюють m-послідовності з максимальним періодом $2k-1$ [17].

Операція XOR ("виключене АБО") – це бінарна логічна операція, яка повертає 1, якщо вхідні біти різні, і 0, якщо однакові.

Таблиця 2

Істинності для операції XOR

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Властивості операції XOR:

комутативність $A \oplus B = B \oplus A$;

асоціативність $(A \oplus B) \oplus C = A \oplus (B \oplus C)$;

ідентичність $A \oplus 0 = A$;

інверсія $A \oplus A = 0$.

Вираз (3) описує рекурентне правило для генерації послідовності в ЛЗРЗЗ, де S_n, S_{n+1},…, S_{n+k} – елементи бінарної послідовності (зазвичай 0 або 1), які представляють стан регістру у момент часу n;

C_1, C_2,…, C_k – коефіцієнти характеристичного многочлена, де кожен $Ci \in \{0,1\}$. Ці коефіцієнти визначають, які попередні стани послідовності впливають на наступний стан. Зазвичай $C_k = 1$ (щоб многочлен був нормалізованим).

k – довжина регістру (кількість бітів або ступінь характеристичного многочлена).

В тому числі вираз (3) показує, що новий стан S_{n+k} обчислюється як результат операції XOR усіх попередніх станів S_{n+k-1}, S_{n+k-2},… S_n, помножені на відповідні коефіцієнти Ci.

Якщо $Ci = 0$, відповідний член ігнорується (тобто не бере участі в операції XOR).

У контексті ЛЗРЗЗ: операція XOR використовується для комбінування бітів із зворотного зв'язку, визначеного коефіцієнтами Ci. Наприклад: якщо $C_1 = 1$ і $C_2 = 1$, то $S_{n+2} = S_{n+1} \oplus S_n$ (зсуваємо і додаємо через операцію XOR).

Нелінійні методи складаються з нелінійних конгруентних генераторів:

$$X_{n+1} = (aX_n^2 + bX_n + c) mod\ m. \quad (4)$$

Вираз (4), де додано квадратичний або вищий член для руйнування лінійності та підвищення ентропії, хаотичних генераторів, базується на нелінійних відображеннях типу:

$$X_{n+1} = rX_n(1 - x_n), \quad X_n \in (0,1), \quad r \in (3.57, 4),$$

де r – параметр хаосу криптографічних генераторів котрі будуються на односторонніх функціях:

$$X_{n+1} = H(X_n \parallel s) \text{ [18]}, \quad (5)$$

де $H(\cdot)$ – криптографічна геш-функція (SHA-2, SHA-3);

s – додатковий параметр, який може виступати в ролі солі (salt) початкового значення (*seed*) або ключа, що визначає результат роботи алгоритму.

Інший варіант – використання потокових шифрів, де ключовий потік виступає ПВП [9].

Вираз (5) складається з кількох компонентів, які потрібно інтерпретувати:

X_n – поточне значення послідовності (може бути числом, рядком бітів або байтів, залежно від контексту);

X_{n+1} – наступне значення послідовності, яке обчислюється;

H – функція, ймовірно, геш-функція (наприклад, SHA-256, MD5), яка перетворює вхідні дані в фіксований вихідний геш;

$\|$ – операція конкатенації (об'єднання), яка з'єднує два елементи (наприклад, X_n і s) в один рядок або послідовність бітів.

Цей вираз описує ітеративний процес генерації послідовності, де кожне наступне значення X_{n+1} залежить від попереднього X_n і фіксованого s, об'єднаних через конкатенацію та оброблених геш-функцію H.

Наприклад: початкове $X_0 = 1001$, $s = 1100$, H – функція, що повертає 8 бітів;

$X_1 = (10011100 = 10101010$ (уявімо, що геш дає цей результат);

$X_2 = (10101010 \| 1100 = H(101010101100)$, і так далі.

Гібридні методи складаються з комбінованих генераторів (приклад – операція XOR-комбінація двох РЗЛЗЗ:

$$s_n = s_n^{(1)} \oplus s_n^{(2)}, \tag{6}$$

де $s_n^{(1)}, s_n^{(2)}$ – виходи двох незалежних регістрів; та методи комбінованих конгруентних генераторів:

$$(X_{n+1} = (a_n X_n \bmod m_1 - a_2 X_n \bmod m_2) \bmod (m_2 - 1), \tag{7}$$

що дозволяє значно подовжити період та зменшити кореляції [16].

Окреме місце займають апаратні методи які реалізуються через фізичні процеси (шум, хаотичні осцилятори).

У спрощеному вигляді формула апаратного генератора може описуватися як:

$$X_{n+1} = \mathrm{Q}(\eta_n), \tag{8}$$

де η_n – виміряний шумовий сигнал;

$Q(\cdot)$ – процедура квантування до бітової форми [19].

Таким чином, формалізація кожного методу через математичні співвідношення дозволяє систематизувати підходи до генерації ПВП. Лінійні методи забезпечують простоту, нелінійні – криптографічну стійкість, гібридні – баланс властивостей, а апаратні – фізичну випадковість та високу швидкодію.

Різноманіття методів генерації зумовило появу великої кількості типів (ПВП), кожен з яких має власні характеристики: довжину періоду, спектральні властивості, рівень кореляції та криптографічну стійкість.

На практиці особливе місце посідають наступні класи (табл. 3).

Таблиця 3

Класифікація ПВП

Класи псевдовипадкових послідовностей					
Максимально довгі послідовності	Голд послідовності	Послідовності Kasami	Збільшені сімейства	Хаотичні послідовності	Криптографічні ключові потоки

Максимально довгі послідовності m-послідовності генеруються регістрами зсуву з лінійним зворотним зв'язком (РЗЛЗЗ) за характеристичним многочленом, що є примітивним над полем GF(2). Їх період дорівнює:

$$T = 2^n - 1, \tag{9}$$

де n – довжина регістра.

Властивості m-послідовностей: рівномірний розподіл нулів і одиниць (різниця не більше ніж на 1), двозначна автокореляційна функція (10) [20]:

$$\mathrm{R}(\tau) = \begin{cases} 1 & \text{при } \tau = 0 \\ -\frac{1}{2^n - 1} & \text{при } \tau \neq 0 \end{cases}. \tag{10}$$

Голд-послідовності отримуються як операція XOR двох різних m-послідовностей з однаковим періодом $2^n - 1$. Їх кількість N становить приблизно $2^n = 1$.

Математично виражається як:

$$g_i(t) = s_i(t) \oplus s_2(t + i), \tag{11}$$

де s_1 ,s_2 – m-послідовності;

i – зсув.

Перевагою є обмеженість значень кореляційної функції (наприклад, $-1, -t(n)$, $t(n) - 2$, що дозволяє використовувати їх у багатокористувальних системах CDMA [21].

Послідовності Kasami формуються на основі підмножини m-послідовностей та характеризуються ще кращими властивостями кореляції.

Для малої підмножини довжина періоду становить:

$$T = 2^n - 1, \tag{12}$$

а кількість послідовностей N дорівнює $2^{n}/_{2}$.

Дані послідовності знаходять застосування у стільникових мережах, супутникових каналах та військових системах зв'язку завдяки низькому рівню взаємної кореляції [22].

Збільшені сімейства такі як:

Коди Уолша: формуються за допомогою матриці Адамара:

$$H_1 = [1],\ H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}. \tag{13}$$

Усі послідовності взаємно ортогональні, що дозволяє застосовувати їх у каналах множинного доступу з ортогональним розділенням [23].

Коди Баркера – короткі послідовності довжиною N, для яких автокореляційна функція задовольняє умову:

$$\mathrm{R}(\tau) \leq 1,\ \tau \neq 0. \tag{14}$$

Використовуються у радіолокації завдяки мінімізації бічних пелюсток кореляційної функції [24].

Хаотичні послідовності формуються за допомогою хаотичних карт, наприклад, логістичного відображення:

$$x_{n+1} = rx_n(1 - x_n),\ x_n \in (1,0). \quad (15)$$

Властивості: непередбачуваність; висока ентропія; можливість регулювати спектральні характеристики.

Хаотичні ПВП все частіше використовуються у криптографії та системах безпілотної техніки [19].

У сучасних системах захисту інформації застосовуються криптографічні генератори, які формують ключові потоки.

Приклад – генератор на основі блочного шифру, що математично представлено формулою (16):

$$S_i = E_k(IV + i), \quad (16)$$

де $E_k(\cdot)$ – шифрування за ключем;
K – ключ шифрування;
IV – ініціалізаційний вектор.

Такі послідовності не тільки володіють статистичними властивостями ПВП, але й гарантують стійкість до атак [9].

Таким чином, типи ПВП різняться за своїми властивостями та областями застосування. m-послідовності та їх узагальнення (Голд, Kasami) ефективні у зв’язку та радіолокації; коди Уолша і Баркера – у сигнальних системах; хаотичні – у сучасних криптографічних протоколах; а криптографічні потоки – в інформаційній безпеці. Це підкреслює важливість грамотного вибору типу послідовності залежно від завдання, що безпосередньо пов’язано з військовою технікою та системами зв’язку.

Серед галузей застосування псевдовипадкових послідовностей найбільший інтерес у дослідників викликає криптографія.

У криптографії ПВП є основою генераторів ключових потоків, шифрів із секретним розподілом ключів та протоколів автентифікації, де необхідна висока ентропія й непередбачуваність [25; 26].

У криптографії справжня випадковість (наприклад, з фізичних джерел, як шум діодів) є ідеальною, але важко генерувати в великих обсягах. Тому використовують ПВП – послідовності, створені детермінованими алгоритмами, які виглядають випадковими, але повторюються при однакових початкових умовах. Вони повинні бути криптостійкими, тобто:

неможливість прогнозування наступного елемента послідовності навіть за умови знання довільної кількості попередніх;

стійкість до криптоаналітичних атак, зокрема методів зворотного відновлення алгоритму;

наявність максимального періоду та відповідність основним статистичним критеріям випадковості, що забезпечує можливість практичного застосування методу.

Генерація криптографічних ключів.

У симетричних криптографічних системах (зокрема, AES, DES) ключ виступає у вигляді бінарної послідовності значної довжини (зазвичай 128–256 бітів), яка визначає процеси шифрування та дешифрування інформаційних потоків.

Формування такого ключа ґрунтується на використанні псевдовипадкових послідовностей (ПВП), що генеруються на основі початкового значення (seed), котре може поєднувати пароль користувача із додатковими параметрами, наприклад, сіллю (salt). З метою

підвищення криптографічної стійкості до отриманої ПВП застосовується криптографічна геш-функція $H(\cdot)$, зокрема SHA-256, у результаті чого формується ключ.

Практичним прикладом є протоколи захисту бездротових мереж (наприклад, WPA2), де ключі формуються з паролів користувача шляхом використання алгоритму PBKDF2, що інтегрує ПВП для забезпечення додаткової ентропії та протидії словниковим атакам.

Ключовим аспектом є те, що без застосування ПВП криптографічні ключі мали б передбачувану структуру, що значно знижувало б рівень захисту і робило систему вразливою до несанкціонованого доступу.

Створення одноразових шифрів.

Одноразові шифри реалізуються шляхом використання псевдовипадкової послідовності, як ключа для операції XOR з повідомленням:

$$C = M \oplus K, \tag{17}$$

де M – вихідне повідомлення;

K – ключ у вигляді ПВП;

C – зашифрований текст [27].

Важливою умовою є те, що ключ повинен мати довжину, ідентичну довжині повідомлення, та використовуватися лише один раз. Порушення цієї вимоги призводить до значного зниження криптографічної стійкості [27; 28].

Прикладом практичного застосування даного принципу є потокові шифри, у яких для кожного пакета даних генерується нова послідовність ключових бітів. Історично застосовувався алгоритм RC4, який сьогодні вважається компрометованим, тоді як сучасні рішення базуються на безпечніших генераторах, таких як Salsa20 та його похідні [28].

Сутність методу полягає у тому, що за умови використання дійсно випадкового, секретного та одноразового ключа забезпечується абсолютна криптографічна стійкість, що теоретично унеможливлює розкриття повідомлення без знання ключа [29].

Вектори ініціалізації та nonce.

Використання векторів ініціалізації та одноразових числових значень (*nonce*) є фундаментальним механізмом забезпечення криптографічної стійкості сучасних систем шифрування [30].

Вектор ініціалізації IV являє собою коротку псевдовипадкову послідовність, яка поєднується з ключем шифру для запобігання появі ідентичних вихідних блоків у різних сеансах. У симетричних алгоритмах, зокрема в режимах Cipher Block Chaining (CBC) та Counter Mode (CTR), додавання IV до ключа забезпечує унікальність криптографічного перетворення для кожного блоку даних [31].

Поняття (*nonce*) передбачає використання унікальної псевдовипадкової послідовності для кожного повідомлення або транзакції в межах криптографічного протоколу. Наприклад, у режимі AES-GCM nonce виступає основою для генерації ключового потоку, що гарантує неможливість повторного застосування однакових параметрів при шифруванні [30; 32].

Фактично, механізм можна подати у виді:

$$IV \oplus K \Rightarrow K^*, \tag{18}$$

де IV – вектор ініціалізації;

K – основний ключ;

K^* – унікальний ключ для поточного блоку чи сеансу.

Практичним прикладом є протокол Transport Layer Security (TLS), що використовується для захищеного передавання даних в Інтернеті: у ньому для кожного сеансу формується унікальний nonce, який генерується псевдовипадковою послідовністю. Це забезпечує захист від атак, що базуються на повторному використанні зашифрованих даних.

Сутність цього підходу полягає в тому, що за відсутності векторів ініціалізації або nonce повторювальні повідомлення залишалися б вразливими для статистичного аналізу, що значно знижувало б рівень безпеки криптографічних систем [30; 32].

Використання солей (*salts*) при гешуванні паролів. Сіль визначається як псевдовипадкова послідовність, яка додається до пароля перед обчисленням його геш-значення. Це дозволяє сформувати унікальний вхідний рядок для криптографічної функції гешування. Процес описується співвідношенням:

$$h = H(P \parallel s), \tag{19}$$

де P – пароль користувача.

У практичних реалізаціях (наприклад, алгоритми *bcrypt, Argon2*) кожному користувачу в системі призначається власна унікальна сіль, завдяки чому навіть ідентичні паролі відображаються у різні геші. Це унеможливлює застосування заздалегідь обчислених таблиць відповідностей та ускладнює словникові атаки.

Сутність даного підходу полягає у підвищенні криптографічної стійкості систем автентифікації за рахунок індивідуалізації результатів гешування та мінімізації ризику компрометації баз даних паролів.

Генерація підписів і випадкових чисел.

У криптографічних системах використання псевдовипадкових послідовностей відіграє ключову роль у забезпеченні надійності цифрових підписів та протоколів обміну ключами. Зокрема, у схемах цифрового підпису, таких як ECDSA та RSA, псевдовипадкові значення застосовуються як *nonce* для запобігання компрометації секретних ключів [33].

У протоколах встановлення спільних параметрів, наприклад, у Diffie–Hellman, псевдовипадкові послідовності використовуються для генерації тимчасових ключів, що забезпечує унікальність та стійкість процесу обміну [34].

Прикладом практичного застосування даного підходу є система Bitcoin, де nonce використовується під час процесу майнінгу. Його роль полягає у варіюванні вхідних даних блоку для пошуку хешу з необхідними криптографічними властивостями, що відповідають встановленому рівню складності [35].

Загалом, використання псевдовипадкових послідовностей гарантує непередбачуваність криптографічних операцій і виключає можливість атак на основі повторів, тим самим підвищуючи безпеку системи [36].

Загальні висновки

Проведений аналіз засвідчив, що псевдовипадкові послідовності мають багатовекторне застосування у військових системах: від формування сигнальних структур у радіозв’язку та радіолокації до забезпечення криптографічних протоколів і процедур автентифікації. Різні класи ПВП демонструють відмінні характеристики – одні орієнтовані на високу швидкодію та простоту реалізації, інші забезпечують підвищений рівень непередбачуваності й стійкість до атак. Узагальнення підходів показало, що ефективність ПВП визначається не лише математичними властивостями, але й їхньою здатністю адаптуватися до вимог конкретних підсистем озброєння. Перспективним напрямом є розробка комбінованих і гібридних генераторів, які поєднують криптографічну стійкість, статистичну якість і технічну ефективність для практичного застосування у складних воєнно-технічних комплексах.

Напрямком подальшого розвитку наукової діяльності доцільно обрати розробку методів генерації створення ПВП для їх застосування у військовій сфері, зокрема в засобах радіозв’язку та електронно-комунікаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малахов О. А. Системи захищеного військового зв’язку. Київ: НУОУ, 2020.

2. Zhang Z., Zhang Y., Xu Z., Wang J. Design and analysis of spreading sequences for secure communications. *IEEE Access.* 2018. Vol. 6. P. 23518–23528. DOI: 10.1109/ACCESS.2018.2833166.

3. Боднар В. П. Захист інформації у системах військового призначення. Харків: ХНУРЕ, 2021.

4. Ding Z., Poor H. V. Design of multi-antenna spectrum sharing systems for wireless communications. *IEEE Transactions on Signal Processing.* 2015. Vol. 63, No. 4. P. 1003–1015. DOI: 10.1109/TSP.2014.2384197.

5. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on post-quantum cryptography. NISTIR 8105. National Institute of Standards and Technology, 2016.

6. Niederreiter H., Winterhof A. Applied number theory. Springer, 2015.

7. Gentle J. E. Random number generation and Monte Carlo methods. Springer Science & Business Media, 2013.

8. Bucci M., Luzzi R., Trifiletti A. A high-speed oscillator-based true random number source for cryptographic applications on a smart card IC. *IEEE Transactions on Computers.* 2010. Vol. 59, No. 11. P. 1543–1554. DOI: 10.1109/TC.2010.125.

9. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev.1. National Institute of Standards and Technology, 2015.

10. Stipčević M., Koç Ç. K. True random number generators. In: Open Problems in Mathematics and Computational Science. Springer, 2014. P. 275–315. DOI: 10.1007/978-3-319-10683-0_13.

11. Li C., Babu P., Palomar D. P. Optimization methods for designing sequences with low autocorrelation sidelobes. *IEEE Transactions on Signal Processing.* 2014. Vol. 62, No. 7. P. 1711–1726. DOI: 10.1109/TSP.2014.2300837.

12. Möller T., Miller D. Uniform distribution measures of pseudorandom sequences in Monte Carlo integration. *Journal of Computational Physics.* 2016. Vol. 307. P. 50–68. DOI: 10.1016/j.jcp.2015.12.038.

13. Li C., Zhang Y., Wang C., Hanzo L. Physical layer security in military wireless networks. *IEEE Transactions on Vehicular Technology.* 2020. Vol. 69, No. 10. P. 11739–11752. DOI: 10.1109/TVT.2020.3016035.

14. Katz D. J. Sequences with low correlation. In: Л. Budaghyan, F. Rodríguez-Henríquez (eds.). *Arithmetic of Finite Fields. WAIFI 2018. Lecture Notes in Computer Science*, vol. 11321. Springer, 2018. P. 149–172.

15.Li C. A survey on complexity measures for pseudo-random sequences. *Cryptography.* 2024. Vol. 8, No. 2. P. 25. DOI: 10.3390/cryptography8020025.

16. L’Ecuyer P. History of uniform random number generation. *ACM Transactions on Modeling and Computer Simulation.* 2017. Vol. 28, No. 1. P. 1–35. DOI: 10.1145/3121434.

17. Wang X., Hu J. A new LFSR-based pseudorandom number generator. *International Journal of Computer Mathematics.* 2012. Vol. 89, No. 16. P. 2141–2152. DOI: 10.1080/00207160.2012.669457.

18. Kocarev L., Stojanovski T. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine.* 2011. Vol. 1, No. 3. P. 6–21. DOI: 10.1109/7384.963463.

19. Sunar B., Martin W. J., Stinson D. R. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers.* 2012. Vol. 56, No. 1. P. 109–119. DOI: 10.1109/TC.2006.257.

20. Canteaut A. LFSR-based Stream Ciphers. MPRI Lecture Notes, 2016.

21. Devrari A. et al. Sequential logic circuit Gold codes: LFSR-based gold code generator chip. *Microprocessors and Microsystems.* 2024. DOI: 10.1016/j.micpro.2024.104825.

22. Jiang W. On the generalized large set of Kasami sequences. *Applied Algebra in Engineering, Communication and Computing.* 2010. Vol. 21. P. 377–389. DOI: 10.1007/s00200-009-0105-3.

23. Wang S. et al. A Walsh-Hadamard coded spectral-efficient full-frequency-diversity COFDM. *IEEE Transactions on Communications.* 2010. Vol. 58, No. 7. P. 1966–1976. DOI: 10.1109/ TCOMM.2010.07.090116.

24. Suesser-Rechberger B., et al. Performance of Walsh-Hadamard codes used for timing recovery in a DVB-S2x multibeam scenario. CSNDSP 2016. DOI: 10.1109/CSNDSP.2016.7573985.

25. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. CRC Press, 2021.

26. Bernstein D. J., Lange T. Post-Quantum Cryptography. Springer, 2017.

27. Cerruti U., Fogliato R., Trovò F. One Time Pad and the Short Key Dream. *arXiv preprint.* 2021. arXiv:2108.06981.

28. Nabil M. A new-one-time-pad stream cipher. *International Journal of Wireless and Mobile Computing.* 2020. Vol. 18, No. 1. P. 46–56. DOI: 10.1504/IJWMC.2020.104364.

29. Ji Z., Xu J., Huang C., Yuen C. Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission. *arXiv preprint.* 2020. arXiv:2010.14268.

30. Kampanakis P. et al. Practical Challenges with AES-GCM and the need for a nonce misuse-resistance option. NIST Workshop on Block Cipher Modes of Operation, 2024.

31. Gueron S. Compound-CTR: Counter Mode for Long Messages and a Long Nonce. *ACM Conference Paper.* 2022. DOI: 10.1145/3510548.3519545.

32. Li H., Wang Y., Ma Y., Jia W., Bai L. AEAD Modes for ZUC Family Stream Ciphers. *arXiv preprint.* 2021. arXiv:2111.05117.

33. Osaki S., Kunihiro N. Bias from Uniform Nonce: Revised Fourier Analysis-based Attack on ECDSA. SAC Workshop 2024. DOI: 10.1007/978-3-031-82852-2_9.

34. National Institute of Standards and Technology. Cryptographic Nonce. 2024.

35. Benkoczi R. et al. Quantum Bitcoin Mining. *Philosophical Transactions of the Royal Society A.* 2022. Vol. 380, No. 2229. P. 20210199. DOI: 10.1098/rsta.2021.0199.

36. Trail of Bits. ECDSA: Handle with Care. Trail of Bits Security Blog. 2020.