https://doi.org/10.31891/2307-5732-2026-363-19
УДК 004.056

ГАВЕЛЬ СЕРГІЙ
Державний університет інтелектуальних технологій і зв'язку, м. Одеса
https://orcid.org/0000-0002-0484-5620
e-mail: arkominer@gmail.com
КОРЧИНСЬКИЙ ВОЛОДИМИР
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
СТЕПАНОВ ВАДИМ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0001-0851-4220
e-mail: stepanovvadym333@gmail.com
КУРТІКОВ МИХАЙЛО
Warner Music Group
https://orcid.org/0009-0002-3537-2624
e-mail: mihajlokurtikov@gmail.com

МЕТОДИ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ГЕНЕРАТОРІВ ХАОСУ

У роботі проведено дослідження методів підвищення криптографічної стійкості псевдовипадкових послідовностей, які формуються за допомогою дискретних генераторів хаосу. Обґрунтована доцільність застосування хаотичних коливань як джерела детермінованої непередбачуваності, що характеризується високою чутливістю до початкових умов, широким спектральним діапазоном і статистичними властивостями, наближеними до випадкових процесів. Застосування такого підходу забезпечує формування послідовностей із підвищеним рівнем ентропії, що є однією з ключових вимог до криптографічних алгоритмів і систем захисту інформації. На основі порівняльного аналізу числових і бітових послідовностей, сформованих за допомогою логістичного відображення у хаотичному режимі, досліджено вплив методів квантування та додаткової обробки на статистичні та кореляційні характеристики псевдовипадкових послідовностей. Показано, що використання середнього значення вибірки як порога квантування дозволяє забезпечити баланс між нулями та одиницями навіть за наявності статистичних відхилень, характерних для практичних реалізацій хаотичних генераторів. Для додаткового ускладнення передбачуваності та покращення спектральних властивостей сформованих послідовностей застосовано операцію циклічного зсуву.

Актуальність роботи обґрунтовується доцільністю застосування хаотичних генераторів у системах захисту інформації, що функціонують в умовах активних радіоелектронних завад і навмисних впливів на канали зв'язку. У таких умовах класичні криптографічні алгоритми потребують доповнення методами, здатними забезпечити як криптографічну стійкість, так і прихованість сигнальних конструкцій. Основними завданнями дослідження є формування псевдовипадкових бітових послідовностей на основі хаотичних відображень, оцінка їх статистичних властивостей, а також аналіз автокореляційних характеристик з метою визначення придатності для криптографічних і телекомунікаційних застосувань. Автокореляційний аналіз підтвердив низький рівень кореляційної залежності і відсутність вираженої періодичності у сформованих послідовностях.

Отримані результати доцільно використовувати під час проєктування криптографічних систем, реалізації технологій розширення спектра, а також розроблення сигнально-кодових конструкцій для захищених каналів зв'язку, у тому числі в умовах активної радіоелектронної боротьби.

Ключові слова: *хаотичні генератори, псевдовипадкові послідовності, криптографічна стійкість, автокореляція, розширення спектра, захист інформації.*

HAVEL SERHII, KORCHYNSKYI VOLODYMYR, STEPANOV VADYM
State University of Intellectual Technologies and Telecommunications
KURTIKOV MYKHAYLO
Warner Music Group

METHODS FOR IMPROVING THE CRYPTOGRAPHIC STRENGTH OF PSEUDORANDOM SEQUENCES BASED ON CHAOTIC GENERATORS

The paper investigates methods for improving the cryptographic strength of pseudorandom bit sequences generated using software-based chaotic generators. The possibility of employing chaotic oscillations as a source of deterministic unpredictability is considered, combining high sensitivity to initial conditions, a wide spectral range, and statistical properties close to those of random processes. This approach makes it possible to generate sequences with increased entropy, which is a key requirement for cryptographic applications. Based on a comparative analysis of numerical and binary sequences formed using the logistic map in the chaotic regime, the influence of quantization methods and additional processing on the statistical and correlation characteristics of pseudorandom sequences is studied. It is shown that the use of the sample mean as a quantization threshold ensures a balance between zeros and ones even in the presence of statistical deviations typical for practical implementations of chaotic generators. To further increase unpredictability and improve the spectral properties of the generated sequences, a cyclic shift operation is applied. The relevance of this research is justified by the expediency of using chaotic generators in information security systems operating under conditions of active electronic countermeasures and intentional interference with communication channels. Under such conditions, classical cryptographic algorithms require enhancement by methods capable of providing both cryptographic strength and concealment of signal structures. The main objectives of the study include the generation of pseudorandom bit sequences based on chaotic mappings, evaluation of their statistical properties, and analysis of autocorrelation characteristics in order to determine their suitability for cryptographic and telecommunication applications. Autocorrelation analysis confirmed a low level of correlation dependencies and the absence of pronounced periodicities in the generated sequences.

The obtained results can be used in the development of cryptographic systems, spread spectrum technologies, as well as signal-code constructions for secure communication channels, particularly under conditions of electronic warfare.

Keywords: *chaotic generators, pseudorandom sequences, cryptographic strength, autocorrelation, spread spectrum, information security.*

Стаття надійшла до редакції / Received 18.01.2026
Прийнята до друку / Accepted 11.02.2026
Опубліковано / Published 26.03.2026

Постановка проблеми

Актуальність дослідження обумовлена стрімким розвитком засобів радіоелектронної боротьби [1], які створюють складні умови для передавання інформації та суттєво підвищують вимоги до прихованості й криптографічної стійкості сигнальних конструкцій [2]. У таких умовах традиційні методи шифрування не завжди забезпечують необхідний рівень захисту, особливо за наявності активного придушення, навмисних завад і перехоплення інформації засобами радіоелектронної розвідки [3]. Отже, важливого значення набуває впровадження нових підходів до формування псевдовипадкових послідовностей (ПВП), які поєднують високий рівень криптографічної стійкості з підвищеною прихованістю та завадостійкістю сигналів [4]. Застосування хаотичних генераторів у цьому контексті розглядається як перспективний напрям, здатний забезпечити ефективний захист від статистичного аналізу, кореляційних атак, а також від впливів, характерних для умов радіоелектронної боротьби. Хаотичні коливання доцільно розглядати як джерело детермінованої непередбачуваності, яке поєднує властивості випадкових процесів із відтворюваністю, необхідною для практичної реалізації криптографічних алгоритмів. Формування хаотичних сигналів може здійснюватися як за допомогою апаратних генераторів, так і шляхом програмної реалізації дискретних хаотичних відображень, що створює передумови для їх ефективного використання у криптографії, технологіях розширення спектра та захищених каналах зв'язку. У зв'язку з цим метою роботи є аналіз і дослідження методів підвищення криптографічної стійкості псевдовипадкових бітових послідовностей, сформованих на основі дискретних генераторів хаосу, з урахуванням вимог до їх статистичних, спектральних і кореляційних характеристик.

Доцільно зазначити, що важливою складовою дослідження є також аналіз сучасних методів оцінювання якості бітових послідовностей, зокрема з використанням ентропійних і автокореляційних показників, які дають змогу обґрунтувати їх придатність для криптографічних і телекомунікаційних застосувань. Основними завданнями роботи є: аналіз методів формування послідовностей на основі хаотичних відображень; дослідження впливу методів квантування та додаткової обробки на статистичні властивості бітових послідовностей; оцінювання автокореляційних характеристик сформованих послідовностей; визначення доцільності використання отриманих ПВП у криптографічних системах і захищених каналах зв'язку, зокрема в умовах радіоелектронної боротьби.

Аналіз останніх джерел

Проблема захисту інформації в умовах радіоелектронних впливів і активних завад широко розглядається в сучасних наукових дослідженнях. Загальні принципи радіоелектронної боротьби (РЕБ), методи впливу на канали зв'язку та способи підвищення завадозахищеності інформаційних систем систематизовано в [1], де визначено ключові напрями протидії радіоелектронним загрозам. Застосування хаотичних сигналів і ПВП для підвищення прихованості передавання інформації було досліджено в [3, 4]. В [5] розглянуто методи формування сигнальних конструкцій на основі хаотичних і таймерних сигналів, а також показано можливість підвищення структурної прихованості систем передавання інформації за рахунок використання хаотичних коливань. У роботі [6] запропоновано підхід до підвищення прихованості передавання інформації на основі мультиплексування таймерних сигналів, що дозволяє зменшити ймовірність виявлення сигналу та підвищити його стійкість до завад.

Фундаментальні основи оцінювання випадковості та ентропії сигналів, що використовуються у криптографічних системах, були закладені в класичних роботах Шеннона [7], де сформульовано математичні критерії інформаційної невизначеності. Теоретичні аспекти завадостійкого кодування, зокрема циклічних кодів і кодів з виправленням помилок, детально описані в працях [8, 9], які залишаються базовими джерелами для аналізу коригувальних властивостей кодових конструкцій. Окремий напрям досліджень присвячений застосуванню хаотичних відображень у криптографії. У працях Девані [10] та Баптісти [11] показано, що дискретні хаотичні системи можуть ефективно застосовуватися для формування криптографічних примітивів завдяки високій чутливості до початкових умов і складній нелінійній динаміці. Подальший розвиток ці ідеї отримали в дослідженнях Альвареса і Лі [12], де проаналізовано криптографічну стійкість хаотичних систем і визначено вимоги до їх практичного застосування.

Отже, аналіз сучасних публікацій свідчить про значний науковий інтерес до використання хаотичних сигналів і завадостійких кодів у системах захисту інформації. Водночас питання комплексної оцінки криптографічних властивостей ПВП, сформованих на основі хаотичних генераторів з урахуванням додаткових операцій обробки, залишаються недостатньо дослідженими, що обумовлює актуальність даної роботи.

Принцип формування псевдовипадкової послідовності на основі програмного генератора хаосу

Розглянемо метод формування бітової послідовності на основі логістичного відображення [3, 4], яке є одним із найпоширеніших дискретних хаотичних відображень:

$$x_{i+1} = ax_i(1 - x_i), \quad (1)$$

де x_i – поточне значення змінної стану, яке належить інтервалу $0 < x_i < 1$; a – керуючий параметр, що визначає характер динаміки системи. За значень $a \in (3{,}57; 4]$логістичне відображення переходить у хаотичний режим, а при $a = 3{,}9$ забезпечується стійкий хаотичний процес із високою чутливістю до початкових умов, що є важливою властивістю для генерації псевдовипадкових послідовностей.

Процес формування ПВП передбачає ітераційне обчислення послідовності чисел $x_1, x_2, \dots, x_N$ після усунення початкового перехідного процесу, який може впливати на статистичні властивості вибірки. Отримана числова послідовність характеризується нерегулярною динамікою та широким спектральним діапазоном, що наближає її властивості до випадкових процесів. Для забезпечення збалансованості бітової послідовності доцільним є визначення середнього значення вибірки:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (2)$$

яке в ідеальному випадку хаотичного режиму прагне до значення, близького до 0,5. Однак у практичних реалізаціях генераторів хаосу можливі статистичні відхилення середнього значення $\bar{x}$, зумовлені обмеженою довжиною вибірки, чисельними похибками обчислень або особливостями початкових умов. Такі відхилення можуть призводити до дисбалансу між кількістю бітів «0» та «1», що негативно впливає на ентропійні характеристики ПВП.

З метою компенсації зазначених ефектів під час побудови генератора доцільно здійснювати контроль та нормалізацію середнього значення вибірки перед етапом квантування. Формування бітової послідовності виконується за наступним правилом порогового перетворення:

$$b_i = \begin{cases} 0, & x_i < \bar{x}, \\ 1, & x_i > \bar{x}. \end{cases} \quad (3)$$

Застосування умови (2) у поєднанні з правилом (3) дозволяє врахувати можливе відхилення середнього значення вибірки $\bar{x}$ від 0,5 та забезпечити близьку до рівноймовірної появу бітів «0» і «1» у сформованій бітовій послідовності b_i. Це, у свою чергу, підвищує ентропію ПВП, зменшує кореляційні залежності між бітами та створює передумови для її використання у криптографічних системах, технологіях розширення спектра та захищених каналах зв'язку.

Методи підвищення криптографічної стійкості псевдовипадкових послідовностей

Для підвищення криптографічної стійкості бітових ПВП, сформованих на основі хаотичних генераторів, доцільним є застосування додаткових операцій обробки, спрямованих на ускладнення прогнозування структури сигналу без погіршення його статистичних характеристик. Одним із таких ефективних методів є операція циклічного зсуву бітової послідовності. Застосування циклічного зсуву дозволяє змінити фазове положення сформованої ПВП, зберігаючи при цьому баланс між кількістю нулів та одиниць, рівень ентропії та спектральні властивості сигналу. Дана операція не змінює статистичного розподілу бітів, проте суттєво ускладнює передбачуваність послідовності та знижує ефективність кореляційного і статистичного криптоаналізу. Алгоритм циклічного зсуву реалізується наступним чином. Нехай задана бітова послідовність

$$B = [b_1, b_2, \dots, b_N] \quad (4)$$

довжиною N, для якої необхідно виконати циклічний зсув. Процедура включає такі етапи:

1) вибір кількості позицій k для зсуву, яка може задаватися випадковим чином або визначатися криптографічним ключем;

2) формування нової бітової послідовності шляхом циклічного лівого зсуву, що описується співвідношенням

$$b'_i = b_{(i+k) \bmod N_j}, \quad (5)$$

де b'_i – біт у новій послідовності після зсуву, а операція $mod\, N_j$забезпечує циклічність перетворення для вибірки довжиною N_j. Отримана після зсуву послідовність $B' = [b'_1, b'_2, \dots, b'_N]$ зберігає статистичні характеристики вихідної ПВП, проте зміна порядку слідування бітів істотно ускладнює її аналіз та відновлення початкової структури без знання параметра зсуву k. Як приклад розглянемо вихідну послідовність

$$B = [1,0,1,1,0,0,1].$$

Після циклічного зсуву на $k = 2$ позиції вліво отримаємо:

$$B' = [1,1,0,0,1,1,0].$$

Для бітової ПВП ентропія визначається за формулою Шеннона [7]:

$$H = -\sum_{i=0}^{1} p_i \log_2 p_i, \quad (6)$$

де p_0 – імовірність появи біта «0», p_1 – імовірність появи біта «1», $p_0 + p_1 = 1$. Максимальне значення ентропії для двійкової послідовності досягається за умови:

$$p_0 = p_1 = 0.5,$$

і дорівнює: $H_{\max} = 1$ біт/символ. Згідно умови (3) алгоритм формування ПВП на основі дискретного генератора хаосу передбачає використання порогу квантування як середнє значення вибірки $\bar{x}$. Це забезпечує наближення частот появи нулів і одиниць до 0,5 навіть за невеликих статистичних відхилень, тобто $p_0 \approx p_1 \approx 0.5$. Отже, можна стверджувати, що ентропія сформованої ПВП близька до максимально можливої. Важливо зазначити, що циклічний зсув не змінює кількість нулів і одиниць, а отже, значення p_0 і p_1 залишаються незмінними. Це

означає, що ентропія після зсуву:

$$H(B') = H(B). \quad (7)$$

Отже, операція зсуву не знижує ентропію, але ускладнює кореляційну структуру, що підвищує криптостійкість ПВП. Для оцінювання статистичних і криптографічних властивостей сформованих ПВП доцільним є застосування автокореляційного аналізу, що дозволяє:

1) виявляти кореляційні залежності між елементами послідовності при різних значеннях зсуву, тобто значення автокореляції, близькі до нуля при $k > 0$, свідчать про відсутність закономірних повторів;

2) оцінювати шумоподібність сигналу, що є критично важливим для задач розширення спектра та забезпечення енергетичної прихованості сигнальних конструкцій, оскільки низька автокореляція забезпечує рівномірний розподіл енергії в частотній області;

3) перевіряти криптографічну якість послідовностей шляхом виявлення прихованої періодичності або структури, здатних знизити криптографічну стійкість.

На рис. 1 наведено автокореляційну функцію $R_{\text{вп}}(k)$ випадкової послідовності, сформованої на основі шумового процесу. Характерною особливістю цієї функції є наявність вираженого піка при нульовому зсуві $k = 0$, що відповідає максимальній кореляції сигналу із самим собою, та значення, близькі до нуля, для всіх ненульових значень зсуву. Така поведінка автокореляційної функції є типовою для білого шуму та свідчить про відсутність статистичних залежностей між елементами послідовності при будь-яких часових зсувах. Це означає, що кожен елемент випадкової послідовності є статистично незалежним від попередніх і наступних, що унеможливлює прогнозування структури сигналу на основі кореляційного аналізу.

На рис. 2 представлено автокореляційну функцію $R_{\text{впвп}}(k)$ хаотичної ПВП, сформованої на основі логістичного відображення (1). Аналіз графіка показує, що, окрім нульового зсуву, значення автокореляції швидко зменшуються до малих, близьких до нуля величин уже при кількох кроках зсуву. Це свідчить про швидку втрату кореляційних залежностей між елементами хаотичної послідовності, незважаючи на детерміновану природу її формування. Відсутність повільно затухаючих або періодичних складових у автокореляційній функції вказує на те, що послідовність не містить прихованих циклів або регулярних структур, які могли б бути використані для криптоаналізу.

Порівняльний аналіз автокореляційних функцій $R_{\text{вп}}(k)$ і $R_{\text{впвп}}(k)$ демонструє якісну подібність між випадковою послідовністю шумового процесу та хаотичною ПВП. Хоча хаотична послідовність формується за детермінованим законом, її автокореляційні характеристики є близькими до характеристик білого шуму, що підтверджує її шумоподібну природу. Незначні коливання автокореляційної функції для ненульових зсувів мають випадковий характер і не свідчать про наявність систематичних залежностей.

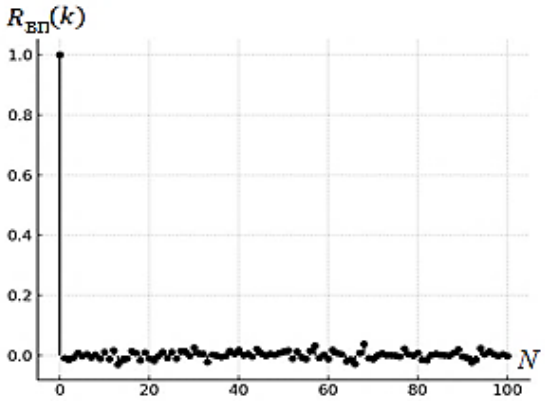

Рис. 1. Автокореляційна функція випадкового процесу $R_{\text{вп}}(k)$

Отримані результати мають принципове значення з погляду забезпечення захисту інформації. Низькі значення автокореляції означають, що сформовані ПВП мають рівномірний розподіл енергії в частотній області, що ускладнює їх виявлення, ідентифікацію та придушення засобами радіоелектронної розвідки і радіоелектронної боротьби. Крім того, відсутність кореляційних залежностей істотно знижує ефективність статистичного та кореляційного криптоаналізу. Отже, аналіз автокореляційних функцій підтверджує, що ПВП, сформовані на основі логістичного хаотичного відображення, за своїми кореляційними та спектральними властивостями наближаються до білого шуму. Це дозволяє розглядати їх як ефективну основу для формування сигнально-кодових конструкцій у криптографічних системах, технологіях розширення спектра та захищених каналах зв'язку, зокрема в умовах активної радіоелектронної боротьби.

Практичне значення автокореляційного аналізу полягає у можливості комплексного оцінювання властивостей ПВП, що використовуються у сучасних системах захисту інформації, телекомунікаційних і криптографічних застосуваннях. У системах стеганографії автокореляційний аналіз дозволяє забезпечити непомітність прихованої інформації за рахунок відсутності регулярних структур і повторів у сигналі, які могли б бути виявлені методами статистичного або кореляційного аналізу, що зменшує ймовірність виявлення факту прихованої передачі даних.

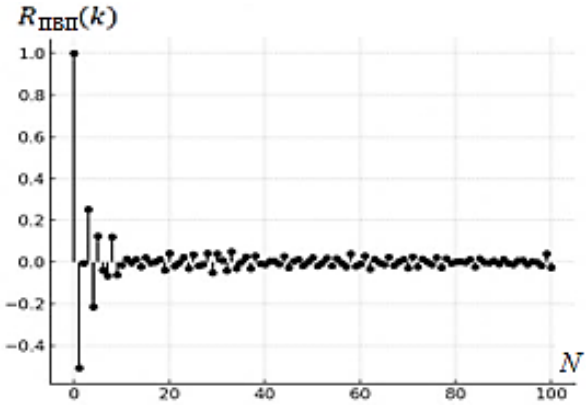

Рис. 2. Автокореляційна функція хаотичної послідовності $R_{\text{впвп}}(k)$ логістичного відображення

У системах радіозв'язку низькі значення автокореляції є важливими для формування завадостійких кодових послідовностей і сигналів із розширеним спектром, оскільки вони забезпечують рівномірний розподіл енергії в частотній області, підвищують стійкість до навмисних і випадкових завад, а також ускладнюють виявлення, ідентифікацію та придушення сигналів засобами радіоелектронної боротьби. У криптографії автокореляційний аналіз застосовується для оцінювання криптографічної якості ПВП, які використовуються у потокових шифрах і генераторах ключових послідовностей, оскільки низький рівень автокореляції свідчить про відсутність прихованих періодичностей і кореляційних залежностей між бітами, що істотно знижує ефективність статистичного та кореляційного криптоаналізу та підвищує загальну криптографічну стійкість систем захисту інформації.

Висновки

У статті проведено дослідження методів підвищення криптографічної стійкості бітових ПВП, сформованих на основі програмних генераторів хаосу. Показано, що використання логістичного відображення у хаотичному режимі дозволяє отримувати числові послідовності з властивостями, близькими до випадкових процесів, що є важливою передумовою для їх застосування у криптографічних системах та захищених каналах зв'язку. Обґрунтовано доцільність застосування середнього значення вибірки як адаптивного порога квантування, що забезпечує баланс між кількістю бітів «0» та «1» і, відповідно, високу ентропію сформованих бітових послідовностей. Встановлено, що такий підхід дозволяє компенсувати статистичні відхилення, характерні для практичних реалізацій хаотичних генераторів. Запропоновано використання операції циклічного зсуву як додаткового засобу підвищення криптографічної стійкості, який не змінює базових статистичних характеристик послідовності, але ускладнює її прогнозування та знижує ефективність кореляційного криптоаналізу. Показано, що застосування циклічного зсуву покращує спектральні властивості ПВП та сприяє формуванню шумоподібних сигналів. Результати автокореляційного аналізу підтвердили низький рівень кореляційних залежностей та відсутність виражених періодичностей у сформованих послідовностях, що свідчить про їх придатність для використання у криптографії, технологіях розширення спектра та формуванні сигнально-кодових конструкцій у системах захисту інформації. Отримані результати можуть бути використані при розробленні засобів криптографічного захисту та інформаційно-комунікаційних систем, зокрема в умовах активної радіоелектронної боротьби.

Література

1. Зайцев Д. В. Основи зв'язку та радіоелектронна боротьба як вид бойового забезпечення : навчальний посібник / Д. В. Зайцев, А. О. Яфонкін, В. В. Ярема ; Університет державної фіскальної служби України. – Ірпінь, 2021. – 280 с.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

3. Корчинський Володимир Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей / Корчинський Володимир, Рябуха Олександр, Аль-Файюмі ХАЛЕД, Гавель Сергій // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах», 2023, № 1 – С. 180-186.

4. Корчинский В. В. Повышение структурной скрытности передачи систем с хаотическими сигналами. – Східно-Європейський журнал передових технологій, № 1/9 (61), 2013, С. 53–57.

5. Захарченко М.В., Корчинский В.В., Радзимовский Б.К. Метод формування сигнальних конструкцій на основі хаотичних і таймерних сигналів у системах передачі конфіденційної інформації. – Збірник наукових праць ОНАЗ ім. О. С. Попова, 2011, № 2, С. 3–7.

6. Korchynskii V. V., Kildishev V. I., Osadchuk E. A. The increase of transmission protection based on multiplexing of timer signal constructions. – Наукові праці ОНАЗ, 2018, № 1, P. 93–97.

7. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423, 623–656.

8. Захарченко М.В., Гаджиєв М.М., Басов В.Є., Мартинова О.М. Системи передавання даних. Т.1: Завадостійке кодування : підручник. Одеса : «Фенікс». 2009. 406 с.

9. Захарченко М.В., Кільдішев В.Й., Мартинова О.М., Ільїн Д.Ю., Трінтіна Н.А. Системи передавання даних. Т.1: Ефективність блокового кодування. Одеса: ОНАЗ ім. О.С. Попова. 2014. 480 с.

10. Devaney R. L. An Introduction to Chaotic Dynamical Systems. — 2nd ed. – Reading, MA: Addison-Wesley, 1989. – 336 p.

11. Baptista M. S. Cryptography with chaos // Physics Letters A. – 1998. – Vol. 240, No. 1–2. – P. 50–54.

12. Álvarez G., Li S. Some basic cryptographic requirements for chaos-based cryptosystems // International Journal of Bifurcation and Chaos. – 2006. – Vol. 16, No. 8. – P. 2129–2151.

References

1. Zaitsev D. V. Osnovy zviazku ta radioelektronna borotba yak vyd boiovoho zabezpechennia : navchalnyi posibnyk / D. V. Zaitsev, A. O. Yafonkin, V. V. Yarema ; Universytet derzhavnoi fiskalnoi sluzhby Ukrainy. – Irpin, 2021. – 280 s.

2. Zakon Ukrainy «Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh». Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31, st. 286. [Elektronnyi resurs]. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

3. Korchynskyi Volodymyr Doslidzhennia variatsiinykh mozhlyvostei heneratoriv khaosu po formuvanniu psevdovypadkovykh poslidovnostei / Korchynskyi Volodymyr, Riabukha Oleksandr, Al-Faiiumi KhALED, Havel Serhii // Mizhnarodnyi naukovo-tekhnichnyi zhurnal «Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh», 2023, № 1 – S. 180-186.

4. Korchinskij V. V. Povyshenie strukturnoj skrytnosti peredachi sistem s haoticheskimi signalami. — Shidno-Yevropejskij zhurnal peredovih tehnologij, № 1/9 (61), 2013, S. 53–57.

5. Zakharchenko M.V., Korchynskyi V.V., Radzymovskyi B.K. Metod formuvannia syhnalnykh konstruktsii na osnovi khaotychnykh i taimernykh syhnaliv u systemakh peredachi konfidentsiinoi informatsii. – Zbirnyk naukovykh prats ONAZ im. O. S. Popova, 2011, № 2, S. 3–7.

6. Korchynskii V. V., Kildishev V. I., Osadchuk E. A. The increase of transmission protection based on multiplexing of timer signal constructions. – Наукові праці ОНАЗ, 2018, № 1, P. 93–97.

7. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423, 623–656.

8. Zakharchenko M.V., Hadzhyiev M.M., Basov V.Ie., Martynova O.M. Systemy peredavannia danykh. T.1: Zavadostiike koduvannia : pidruchnyk. Odesa : «Feniks». 2009. 406 s.

9. Zakharchenko M.V., Kildishev V.I., Martynova O.M., Ilin D.Iu., Trintina N.A. Systemy peredavannia danykh. T.1: Efektyvnist blokovoho koduvannia. Odesa: ONAZ im. O.S. Popova. 2014. 480 s.

10. Devaney R. L. An Introduction to Chaotic Dynamical Systems. — 2nd ed. – Reading, MA: Addison-Wesley, 1989. – 336 p.

11. Baptista M. S. Cryptography with chaos // Physics Letters A. – 1998. – Vol. 240, No. 1–2. – P. 50–54.

12. Álvarez G., Li S. Some basic cryptographic requirements for chaos-based cryptosystems // International Journal of Bifurcation and Chaos. – 2006. – Vol. 16, No. 8. – P. 2129–2151.