

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ
ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ**

Кваліфікаційна наукова
праця на правах рукопису

Кільдішева Віталія Йосиповича

УДК 004.056.53

ДИСЕРТАЦІЯ

**МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ
ПАРАМЕТРИЧНОГО ПЕРЕТВОРЕННЯ ПЕРЕДАВАНИХ СИГНАЛЬНО-
КODOBИХ КОНСТРУКЦІЙ**

05.13.21 – Системи захисту інформації
05 «Технічні науки»

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

 В.Й. Кільдішев

Науковий консультант Корчинський В.В., д. т. н., професор

Ідентичність всіх примірників дисертації

ЗАСВІДЧУЮ:

*В.о. вченого секретаря спеціалізованої
вченої ради*



М.М. Гаджиєв

Одеса–2025

АНОТАЦІЯ

Кільдішев В.Й. Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Державний університет інтелектуальних технологій і зв'язку МОН України, м. Одеса, 2025.

Дисертація присвячена розв'язанню науково-технічної проблеми підвищення захищеності передавання інформації шляхом розробки математичних моделей і методів параметричного перетворення сигнально-кодових конструкцій. Запропоновані підходи до формування шумоподібних таймерних сигналів і побудови багаторівневого захисту інформації забезпечують підвищення прихованості та завадостійкості систем зв'язку в умовах радіоелектронного впливу.

Метою дисертаційної роботи є розв'язання науково-технічної проблеми підвищення захищеності передаваної інформації в інформаційно-комунікаційних системах шляхом розробки моделей та методів параметричного перетворення сигнально-кодових конструкцій, що забезпечують підвищену завадостійкість, прихованість та стійкість до несанкціонованого доступу.

Об'єктом дослідження є процеси формування та інтеграції методів захисту інформації в сигнально-кодових конструкціях для забезпечення прихованості під час передавання в інформаційно-комунікаційних системах.

Предметом дослідження є методи та алгоритми параметричного перетворення сигнально-кодових конструкцій, спрямовані на підвищення прихованості та завадостійкості передавання інформації в умовах радіоелектронного конфлікту.

У вступі розкрито сутність і стан наукової проблеми та обґрунтовано її актуальність, визначено мету роботи й коло вирішених завдань, показано наукову новизну та практичну значущість одержаних результатів, наведено інформацію про особистий внесок здобувача, апробацію та впровадження наукових

результатів роботи.

У *першому розділі* проаналізовано сучасні підходи до захисту інформаційно-комунікаційних систем з позицій завадостійкості, прихованості та криптографії. Обґрунтовано доцільність побудови узагальненої моделі оцінки рівня захищеності передачі інформації з урахуванням параметрів каналу та граничних умов його функціонування. Сформульовано концепцію багаторівневого захисту на основі енергетичної, структурної та інформаційної прихованості, визначено ключові параметри сигналів та запропоновано модель обсягу сигналу як інтегральний критерій захищеності. Систематизовано методи розширення спектра сигналів (ПРС, ППРЧ, ЛЧМ) та показано їх ефективність для зниження спектральної помітності. Розроблено підхід до параметричного перетворення сигнально-кодових конструкцій, що забезпечує адаптивне узгодження між завадостійкістю, прихованістю та ефективністю використання каналу.

У *другому розділі* проведено аналіз процесів передавання інформації в нестационарних каналах зв'язку з урахуванням змінних характеристик середовища. Розглянуто адаптивний обмін між якістю та швидкістю передачі залежно від стану каналу, використання таймерних сигнальних конструкцій для «хороших» інтервалів та розрядно-цифрових кодів для відновлення достовірності. Запропоновано підхід, який компенсує надлишковість блокових кодів за рахунок запасу завадостійкості каналу та оптимізації структури таймерних сигналів, що дозволяє динамічно регулювати співвідношення швидкості і якості передачі та підвищує ефективність системи в умовах радіоелектронного впливу.

У *третьому розділі* досліджено підвищення завадостійкості та структурної прихованості сигнально-кодових конструкцій через варіативне налаштування параметрів таймерного кодування. Показано ефективність поєднання таймерних сигналів з позиційним завадостійким кодуванням і стохастичним шифруванням для компенсації надлишковості елементів. Встановлено зворотну залежність між структурною прихованістю та

завадостійкістю; для її усунення запропоновано використання ансамблю таймерних сигнальних конструкцій, що забезпечує баланс між достовірністю, прихованістю та стійкістю до завад.

У четвертому розділі розроблено багаторівневу модель захисту інформації, що поєднує статистичне шифрування, завадостійке кодування, таймерне перетворення та декореляцію помилок, забезпечуючи одночасне підвищення криптографічної стійкості, достовірності передачі та захисту від несанкціонованого доступу. Обґрунтовано взаємозв'язок параметрів кодових і шифрувальних перетворень із критеріями захищеності, показано підвищення ентропії шифрограм при статистичному шифруванні та ефективність таймерних сигналів для компенсації надлишковості, збільшення структурної прихованості та стійкості до групових помилок.

У п'ятому розділі досліджено параметри таймерних сигналів і їх застосування для формування шумоподібних сигнально-кодових конструкцій. Варіювання параметрів n , s , i та Δ дозволяє керувати спектральними та кореляційними характеристиками сигналів для оптимального балансу між завадостійкістю, прихованістю та пропускнуою здатністю. Проведено порівняльний аналіз алгоритмів розширення спектра, який підтвердив перевагу таймерних конструкцій у забезпеченні структурної прихованості. Розроблено алгоритми синтезу псевдовипадкових послідовностей на основі хаотичних відображень, що підвищують криптографічну стійкість, а використання комбінованих хаотичних генераторів і хешування параметрів забезпечує додатковий рівень захисту. Отримані результати підтверджують ефективність таймерних сигналів і хаотичних систем для забезпечення високого рівня завадостійкості та структурної прихованості каналів зв'язку.

У шостому розділі розроблено та досліджено методи формування шумоподібних таймерних сигналів, спрямованих на забезпечення високого рівня енергетичної та структурної прихованості в умовах радіоелектронного впливу. Показано, що поєднання таймерних сигналів із методами прямого розширення спектра, ППРЧ, ЛЧМ, мультиплексування та хаотичних коливань

формує широкий клас сигналів із підвищеною завадостійкістю. Встановлено, що вибір бази сигналу та алгоритму розширення спектра визначає рівень структурної прихованості та еквівалентної криптостійкості системи. Моделювання підтвердило ефективність комбінованих методів (ТСК та ПВП, ТСК та ППРЧ, ТСК та ЛЧМ), які забезпечують збільшення структурної прихованості у 1,5–2 рази та збереження достовірності передавання при низьких відношеннях сигнал/шум. Запропонований підхід до мультиплексування таймерних сигналів дозволяє зменшити кількість піднесучих частот порівняно з OFDM, водночас підвищивши прихованість і стійкість до завад.

У висновках викладено основні результати проведених досліджень.

Наукова новизна одержаних результатів полягає в такому:

1. Уперше запропоновано модель оцінювання захищеності передачі інформації на основі обсягу сигналу, що забезпечує визначення рівня енергетичної, структурної та інформаційної прихованості з урахуванням характеристик каналу зв'язку.

2. Уперше розроблено метод взаємного обміну якості та швидкості передавання інформації шляхом комбінованого використання таймерних і позиційних кодів у нестаціонарних каналах, що підвищує ефективність і стійкість систем зв'язку в умовах радіоелектронного впливу.

3. Запропоновано метод одночасного захисту від НСД та випадкових завад, який встановлює залежність між структурною прихованістю таймерних сигналів, завадостійкістю та мінімальною кодовою відстанню дозволених комбінацій.

4. Розроблено багаторівневу модель захисту інформації, що поєднує статистичне шифрування, завадостійке та таймерне кодування й декореляцію помилок, забезпечуючи синергетичне підвищення криптостійкості, достовірності та захисту від НСД.

5. Встановлено закономірності впливу параметрів таймерних сигналів на рівень структурної прихованості та завадостійкості. Обґрунтовано критерії

вибору оптимальних параметрів, які забезпечують баланс між складністю реалізації, пропускнуою здатністю та прихованістю.

6. Розвинуто теорію систем зв'язку з шумоподібними сигналами шляхом створення нових методів розширення спектра непозиційних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ) і визначення умов енергетичної прихованості за критеріями частотної та енергетичної ефективності.

Практичне значення одержаних результатів полягає в тому, що розроблені методи та алгоритми забезпечують підвищення ефективності захисту інформації та завадостійкості каналів зв'язку.

1. Запропоновано алгоритм адаптивного обміну між завадостійкістю та швидкістю передачі, який дозволяє вдвічі скоротити час передавання даних у нестационарних каналах.

2. Розроблено метод формування таймерних сигналів із варіативними параметрами, що підвищує структурну прихованість у десятки разів порівняно з позиційними кодами.

3. Створено багаторівневу модель захисту інформації, яка поєднує стохастичне шифрування, завадостійке та таймерне кодування й забезпечує захист від НСД і завад без втрати достовірності.

4. Обґрунтовано методи вибору параметрів таймерних сигналів для формування шумоподібних конструкцій із заданим рівнем прихованості та пропускнуою здатністю.

5. Розроблено алгоритми розширення спектра таймерних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ), які підвищують енергетичну та структурну прихованість, досягаючи рівня криптостійкості, співставного з протоколами DES та AES.

Результати дослідження можуть бути використані при розробці захищених систем зв'язку, апаратно-програмних комплексів шифрування та засобів протидії РЕБ.

Ключові слова: несанкціонований доступ, прихованість, завадостійкість, криптостійкість, радіоелектронна боротьба, перехоплення сигналу, завада, таймерні сигнали, шумоподібний сигнал, розширення спектра, кореляційний

приймач, статистичне шифрування, декореляція помилок.

ABSTRACT

Kildishev V.Y. Models and Methods for Information Protection Based on Parametric Transformation of Transmitted Signal-Code Structures. – Qualification scientific work in manuscript form.

Dissertation for the degree of Doctor of Technical Sciences in the specialty 05.13.21 – Information Security Systems. State University of Intellectual Technologies and Telecommunications, Ministry of Education and Science of Ukraine. – Odessa, 2025.

The dissertation is devoted to solving the scientific and technical problem of increasing the security of information transmission through the development of mathematical models and methods for parametric transformation of signal-code structures. The proposed approaches to forming noise-like timer signals and building a multi-level information protection system ensure increased concealment and noise immunity of communication systems under conditions of electronic warfare.

The aim of the dissertation is to solve the scientific and technical problem of improving the security of transmitted information in information and communication systems by developing models and methods for parametric transformation of signal-code structures, ensuring increased noise immunity, concealment, and resistance to unauthorized access.

The object of the study is the processes of formation and integration of information protection methods in signal-code structures to ensure concealment during transmission in information and communication systems.

The subject of the study is the methods and algorithms of parametric transformation of signal-code structures aimed at increasing the concealment and noise immunity of information transmission under conditions of electronic warfare.

The introduction presents the essence and state of the scientific problem and substantiates its relevance, defines the purpose of the work and the scope of solved tasks, highlights the scientific novelty and practical significance of the obtained

results, and provides information on the personal contribution of the author, as well as the testing and implementation of the scientific results.

Chapter 1 analyzes modern approaches to the protection of information and communication systems from the perspective of noise immunity, concealment, and cryptography. The feasibility of building a generalized model for assessing the level of information transmission protection is substantiated, taking into account the channel parameters and operating limits. The concept of multi-level protection based on energy, structural, and information concealment is formulated, key signal parameters are determined, and a signal volume model is proposed as an integral criterion for protection. Methods for signal spectrum spreading (DSSS, FHSS, LFM) are systematized, and their effectiveness in reducing spectral visibility is demonstrated. An approach to parametric transformation of signal-code structures is developed, providing adaptive coordination between noise immunity, concealment, and channel efficiency.

Chapter 2 analyzes information transmission processes in non-stationary communication channels considering variable environmental characteristics. Adaptive exchange between transmission quality and speed depending on the channel state, the use of timer signal structures for "good" intervals, and digital-rank codes for restoring reliability are considered. An approach is proposed that compensates for the redundancy of block codes by utilizing the channel's noise immunity reserve and optimizing the timer signal structure, allowing dynamic regulation of the speed-quality ratio and increasing system efficiency under electronic warfare conditions.

Chapter 3 investigates the improvement of noise immunity and structural concealment of signal-code structures through variable timer coding parameters. The effectiveness of combining timer signals with position-based error-resistant coding and stochastic encryption to compensate for element redundancy is demonstrated. A reverse relationship between structural concealment and noise immunity is established; to resolve this conflict, the use of an ensemble of timer signal structures is proposed, ensuring a balance between reliability, concealment, and resistance to interference.

Chapter 4 develops a multi-level information protection model combining statistical encryption, error-resistant coding, timer transformation, and error decorrelation, ensuring simultaneous improvement of cryptographic strength, transmission reliability, and protection against unauthorized access. The relationship between coding and encryption parameters and protection criteria is substantiated, showing increased ciphertext entropy in statistical encryption and the effectiveness of timer signals in compensating redundancy, increasing structural concealment, and resistance to grouped errors.

Chapter 5 studies the parameters of timer signals and their application in forming noise-like signal-code structures. Varying the parameters n , s , i , and Δ allows control over the spectral and correlation characteristics of signals for an optimal balance between noise immunity, concealment, and system throughput. A comparative analysis of spectrum spreading algorithms confirmed the advantage of timer structures in ensuring structural concealment. Algorithms for synthesizing pseudorandom sequences based on chaotic maps are developed to enhance cryptographic strength, and the use of combined chaotic generators and parameter hashing provides an additional level of protection. The results confirm the effectiveness of timer signals and chaotic systems in achieving high noise immunity and structural concealment in communication channels.

Chapter 6 develops and investigates methods for forming noise-like timer signals aimed at ensuring high levels of energy and structural concealment under electronic warfare conditions. It is shown that combining timer signals with direct spectrum spreading methods, FHSS LFM, multiplexing, and chaotic oscillations forms a wide class of signals with enhanced noise immunity. The choice of signal base and spectrum spreading algorithm determines the level of structural concealment and equivalent cryptographic strength. Modeling confirmed the effectiveness of combined methods (TSC & FHSS, TSC & DSSS, TSC & LFM), which increase structural concealment by 1.5–2 times and maintain transmission reliability under low signal-to-noise ratios. The proposed approach to timer signal multiplexing reduces the number of carrier frequencies compared to OFDM while increasing concealment

and noise resistance.

Conclusions summarize the main results of the study.

Scientific novelty of the obtained results:

1. A signal-volume-based model for assessing information transmission protection is proposed for the first time, allowing determination of energy, structural, and information concealment levels considering channel characteristics.

2. A method of mutual exchange between transmission quality and speed using combined timer and position codes in non-stationary channels is proposed for the first time, increasing communication system efficiency and stability under electronic warfare.

3. A method for simultaneous protection against unauthorized access and random interference is proposed, establishing the relationship between timer signal structural concealment, noise immunity, and minimum code distance of allowed combinations.

4. A multi-level information protection model combining statistical encryption, error-resistant and timer coding, and error decorrelation is developed, ensuring synergistic enhancement of cryptographic strength, reliability, and protection against unauthorized access.

5. Regularities in the influence of timer signal parameters on structural concealment and noise immunity are established, with criteria for selecting optimal parameters to balance implementation complexity, throughput, and concealment.

6. The theory of communication systems with noise-like signals is developed through new methods of non-positional signal spectrum spreading (DSSS, FHSS, LFM) and determination of energy concealment conditions based on frequency and energy efficiency criteria.

Practical significance: The developed methods and algorithms improve information protection efficiency and communication channel noise immunity.

1. An adaptive exchange algorithm between noise immunity and transmission speed is proposed, halving data transmission time in non-stationary channels.

2. A method for forming timer signals with variable parameters is developed,

increasing structural concealment by an order of magnitude compared to position codes.

3. A multi-level information protection model combining stochastic encryption, error-resistant, and timer coding is created, ensuring protection against unauthorized access and interference without loss of reliability.

4. Methods for selecting timer signal parameters to form noise-like structures with specified concealment and throughput are substantiated.

5. Timer signal spectrum spreading algorithms (DSSS, FHSS, LFM) are developed, enhancing energy and structural concealment to cryptographic levels comparable to DES and AES protocols.

The results can be applied in developing secure communication systems, hardware-software encryption complexes, and electronic warfare countermeasure tools.

Keywords: unauthorized access, concealment, noise immunity, cryptographic strength, electronic warfare, signal interception, interference, timer signals, noise-like signal, spectrum spreading, correlation receiver, statistical encryption, error decorrelation.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковано основні наукові результати:

1. Сталий розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б. В. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. Одеса : ДУ «ІРЕЕД НАНУ», 2024. 543 с.

2. Korchynskiy V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaioni Kh. Method of information protection based on the integration of probabilistic encryption and noise immune coding. *Radioelectronic and Computer Systems*. 2023. Vol. 4, No. 13. P. 184-196.

3. Корчинський В. В., Кільдішев В. Й., Онищук В. В., Аль-Файюми Халед. Дослідження ефективності застосування гомоморфних криптосистем у

рекомендаційних системах веб-сервісів. *Інфокомунікаційні та комп'ютерні технології*. 2021. № 2 (02). С. 195–201.

4. Korchynskiy V. V., Kildishev V. I., Alfaion K. та інші. A method for formation parameters of chaos generators based on hash functions. *Наукові праці ОНАЗ*. 2020. № 2. Р. 65-69.

5. Korchynskiy V., Kildishev V., Riabukha O., Berdnikov O. The generating random sequences with the increased cryptographic strength. *Informatics, Automatics and Control Systems*. 2020. No. 1. P. 20-23. – DOI: [10.35784/iapgos.916](https://doi.org/10.35784/iapgos.916) (Scopus).

6. Hordiichuk V., Shyshatskiy A., Korchynskiy V., Kildishev V. Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems. *Journal of Physics: Conference Series*. 2021. Vol. 1839. P. 1-10. DOI: <https://doi.org/10.1088/1742-6596/1839/1/012005> (Scopus).

7. Korchynskiy V. V., Kildishev V. I., Berdnikov A. M., Smazhenko K. O. Increase of stealth transmission based on timer signals and linear frequency modulation. *Наукові праці ОНАЗ ім. О. С. Попова*. 2020. № 1. Р. 53-57.

8. Korchynskiy V. V., Kildishev V. I., Holey D. V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding. *Radio Electronics, Computer Science, Control*. 2019. No. 3 (50). P. 108-116. (Web of Science).

9. Korchynskiy V. V., Kildishev V. I., Berdnikov A. M., Bielova I. V. Methods for generating noise-like timer signals based on pseudo-random tuning of the operating frequency. *Наукові праці ОНАЗ ім. О. С. Попова*. 2019. № 2. С. 98-103.

10. 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. Р. 93-97.

11. Корчинський В. В., Кільдішев В. Й., Осадчук К. О., Бердніков О. М. Дослідження енергетичної прихованості шумоподібних таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ». Серія : Нові рішення в сучасних технологіях*.

2018. № 42 (1214). С. 126-130. DOI: <https://doi.org/10.20998/2413-4295.2018.12.01>.

12. Korchynskiy V. V., Kildishev V. I., Holey D. V., Berdnikov A. M. Research methods of increasing the security of information transfer based on timer signals. *Наукові праці ОНАЗ ім. О. С. Попова*. 2018. № 2. С. 109-115.

13. Корчинський В. В., Кільдішев В. Й., Бердніков О. М., Осадчук К. О. Підвищення захищеності системи зв'язку з таймерними сигнальними конструкціями та псевдовипадковою перебудовою робочої частоти. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 2. С. 179-182.

14. Korchynskii V. V., Kildishev V. I., Berdnikov A. M. Methods for assessing the security of communication systems for special purposes. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 2. Р. 101-107.

15. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Толкачов А. В. Ефективність двосимвольних ансамблів у симплексних системах на базі коригувальних таймерних сигнальних конструкцій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 1. С. 215-218.

16. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Осадчук К. О. Інформаційні параметри кодів Сліп'яна з компенсацією надмірності таймерними сигналами. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 1. С. 14-20.

17. Korchynskii V. V., Osadchuk E. A., Kildishev V. I. Method of multiplexing of timer signal structures based on OFDM technology. *Вісник Національного університету «Львівська політехніка»*. 2017. № 2. Р. 41-44.

18. Стайкуца С. В., Кільдішев В. Й. Ідентичність об'єктів інформаційної мережі як елемент моделі кібербезпеки. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2016. № 2. С. 185-189.

19. Захарченко М. В., Корчинський В. В., Радзімовський Б. К., Кільдішев В. Й. Підвищення скритності передачі конфіденційної інформації на базі хаотичних сигналів та таймерних сигнальних конструкцій. *Східноєвропейський*

журнал передових технологій. 2012. № 3/9 (57). С. 45-49. DOI: <https://doi.org/10.15587/1729-4061.2012.4168>.

20. Корчинський В. В., Кільдішев В. Й., Хомич С. В., Белова Ю. В. Ефективність j -кратного повторення надлишкових таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ»*. 2012. Вип. 26. С. 88-95.

21. Захарченко М. В., Кільдішев В. Й., Белова Ю. В., Хомич С. В. Вплив корельованих завад на пропускну здатність безперервного каналу зв'язку. *Вісник НТУ «ХПІ». Серія : Нові рішення у сучасних технологіях*. 2012. Вип. 33. С. 62-68.

22. Захарченко М. В., Кільдішев В. Й., Хомич С. В., Пришляк О. Г. Компенсація надлишковості в блокових коректуючих кодах за рахунок таймерних сигналів. *Вісник Хмельницького національного університету*. 2011. Вип. 2. С. 175-181.

23. Шевцов Ю. С., Кононович В. Г., Кільдішев В. Й. Модель спільного використання системи виявлення і обробки атак із системою постійного аудиту інформаційної безпеки. *Вісник Східноукраїнського національного університету ім. В. Даля*. 2010. № 9 (151), ч. 1. С. 52-58.

Наукові праці, які засвідчують апробацію матеріалів дисертації

24. Hordiichuk V., Korchynskyi V., Kildishev V., Molodetskyi B., Staikutsa S., Alfaiomi K. Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare. *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv, Ukraine, 2024. P. 1–4. doi:10.1109/TCSET64720.2024.10755658. (Scopus).

25. Кільдішев В.Й. Система оцінок захищеності методів захисту інформації в умовах РЕБ. *Забезпечення кібероборони держави : збірник матеріалів IV наук.-практ. вебінару* (м. Київ, 10 листопада 2023 р.). Київ: НУОУ, 2023. С. 65-68.

26. Onyshchuk V., Kildishev V., Korchynskyi V., Alfaiomi K. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web

Services. *Proc. 16th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 22–26 Feb. 2022. P. 331-334. (Scopus).

27. Hordiichuk V., Korchynskyi V., Kildishev V., Zakharchenko M. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods. *2022 IEEE 2nd Ukrainian Microwave Week (UkrMW)*. Kyiv, 14-18 Nov. 2022. P. 331-334. (Scopus).

28. Корчинський В.В., Кільдішев В.Й., Аль-Файюми Х., Валігурський Ю.П. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції. *Перспективні напрямки захисту інформації: матеріали VII міжнар. наук.-практ. конф.* (м. Одеса, 30 серпня – 3 вересня 2021 р.). Одеса–Тернопіль: Крок, 2021. С. 31-33.

29. Korchynskyi V., Kildishev V., Golev D. Increase of Transmission Security Based on Timer Signal Construction. *2018 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. Odessa, 10–14 Sept. 2018. P. 1-4. doi:10.1109/UkrMiCo43733.2018.9047554. (Scopus).

30. Корчинський В.В., Кільдішев В.Й., Онищук В.В., Аль-Файюми Х. Підвищення захищеності користувацьких даних веб-серверів шляхом впровадження гомоморфного шифрування. *Матеріали 75-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей*. Одеса: ОНАЗ, 2020. С. 132–133.

31. Korchynskyi V., Kildishev V., Berdnikov O., Valihurskyi Y., Polyshchuk K. The Methods of Forming Random Sequences Based on the Dynamic Chaos. *VIII Міжнародна наук.-практ. конф. «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах»* (м. Чернівці, 3–5 жовтня 2019 р.). Чернівці, 2019. С. 26-29.

32. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Губін А.В. Системи радіозв'язку із шумоподібними таймерними сигналами. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів, тези доповідей*. Одеса: ОНАЗ, 2018. С. 134-136.

33. Корчинський В.В., Кільдішев В.Й., Голев Д.В. Прихованість та завадостійкість передачі інформації на основі випадкового таймерного кодування. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей.* Одеса: ОНАЗ, 2018. С. 133-134.

34. Zakharchenko M., Korchynskyi V., Kildishev V. Integrated Methods of Information Security in Telecommunication Systems. *2017 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017).* Odessa, 11–15 Sept. 2017. V.1. P. 78-81. (Scopus).

35. Корчинський В.В., Кільдішев В.Й. Захищеність систем зв'язку спеціального призначення. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (13-15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 18-19.

36. Корчинський В.В., Кільдішев В.Й. Підвищення прихованості передачі в системі зв'язку з кодовим розділенням каналів на основі динамічного хаосу. *XIX Міжнар. наук.-практ. конф. «Безпека інформації у інформаційно-телекомунікаційних системах»* (м. Буча, 25–26 травня 2017 р.). Буча: Держспецзв'язок, 2017. С. 48.

37. Корчинський В. В., Кільдішев В. Й., Бердніков О. М. Методи розширення спектру таймерних сигналів на основі псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали IV Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 57-59.

38. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Валігурський Ю.П. Метод порівняльного аналізу генераторів псевдовипадкових чисел. *Перспективні напрями захисту інформації: матеріали IV Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 46-48.

39. Корчинський В.В., Кільдішев В.Й., Осадчук К.О., Русаловська О.А. Підвищення захищеності передачі інформації на основі таймерних сигнальних конструкцій та технології OFDM. *Перспективні напрями захисту інформації :*

матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 39-42.

40. Кільдішев В.Й., Бердніков О.М., Степанов В.О. Підвищення захищеності системи зв'язку з ППРЧ на основі таймерних сигнальних конструкцій. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (м. Черкаси, 13–15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 17-18.

41. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Русаловська О.А. Спектральні методи захисту інформації на основі таймерних сигналів та псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали III Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 36–39.

42. Корчинський В.В., Кільдішев В.Й., Бердніков О.М. Методи підвищення захищеності систем зв'язку на основі таймерних сигналів. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей.* Одеса: ОНАЗ, 2017. С. 114-117.

43. Корчинський В.В., Кільдішев В.Й., Валігурський Ю.П., Поліщук К.В. Підвищення ефективності потокового шифрування в радіомережах на основі динамічного хаосу. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей.* Одеса: ОНАЗ, 2017. С. 117-118.

44. Захарченко М.В., Корчинський В.В., Кільдішев В.Й. Про доцільність застосування зворотного зв'язку в системах передачі даних. *Матеріали 64-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів* (м. Одеса, 1–4 грудня 2009 р.). Одеса: ОНАЗ, 2009. С. 78-80.

ЗМІСТ

ВСТУП	23
1 Стан проблеми забезпечення завадозахищеності конфіденційної інформації у мережах зв'язку. Вибір напрямку досліджень.....	37
1.1. Теоретичне обґрунтування захисту інформації на основі показників прихованості та завадостійкості	37
1.2. Захист інформації на основі методів розширення спектра сигналу.....	42
1.2.1. Метод прямого розширення спектра	42
1.2.2. Метод розширення спектра на основі псевдовипадкового перескоку робочої частоти	43
1.2.3. Метод розширення спектра на основі лінійної частотної модуляції	49
1.2.4. Забезпечення структурної прихованості сигнальних конструкцій .	51
1.2.5. Забезпечення інформаційної прихованості даних	54
1.3. Вплив параметричного перетворення сигнально-кодових конструкцій на захист інформації	57
1.4. Модель оцінювання захищеності передачі інформації на основі обсягу сигналу	60
1.5. Ресурси каналу зв'язку та умови забезпечення захищеності інформаційно-комунікаційних систем	66
1.5.1. Вплив засобів РЕБ на ресурсні вимоги і захищеність каналів зв'язку	66
1.5.2. Система оцінювання захищеності методів захисту інформації	69
1.6. Розвиток методів підвищення прихованості та завадостійкості сигнальних конструкцій в умовах радіоелектронного протидіювання	78
1.7. Постановка задач на дослідження	80
Висновки	83
2 Підвищення завадостійкості передавання даних на основі сумісного використання блокових завадостійких кодів та таймерних	

сигналів в системах захисту інформації	85
2.1. Огляд математичних моделей дискретного каналу з точки зору придатності до умов РЕБ	85
2.2. Вплив надлишковості на ефективність завадостійкого обміну даними	91
2.3. Обґрунтування адаптивного обміну запасу якості передавання інформації на швидкість	94
2.4. Кореляційна залежність міжсимвольних завад та інформаційних сигналів	99
2.5. Вплив корельованих завад на пропускну здатність безперервного каналу	103
2.6. Компенсація надлишковості в блокових завадостійких кодах за допомогою таймерних сигналів	108
2.7. Інформаційні параметри кодів Слепяна з компенсацією надлишковості таймерними сигналами	119
2.8. Підвищення ефективності використання інтервалу реалізації коду Слепяна	125
Висновки	127
3 Захист інформації на основі непозиційних таймерних сигнальних конструкцій	129
3.1. Захисту інформації від несанкціонованого доступу на основі структурної прихованості сигнальних конструкцій	129
3.2. Аналіз позиційного та непозиційного кодування для забезпечення структурної прихованості сигнально-кодових конструкцій	133
3.3. Оцінка структурної прихованості та мінімальної кодової відстані при виборі реалізацій таймерних сигналів методом перебору	143
3.4. Вплив рівняння якості при таймерному кодуванні на рівень структурної прихованості та завадостійкості	146
3.5. Захист інформації на основі j -кратного повторення надлишкових таймерних сигналів	150
Висновки	161

4 Підвищення захищеності інформації на основі

інтегрованих методів перетворення даних	163
4.1. Обґрунтування комбінованих методів шифрування і кодування	163
4.2. Структура захисту інформації на основі трьох перетворювачів	168
4.3 Взаємозв'язок між рівнями перетворення та критеріями захищеності	173
4.4. Принципи формування шифрограм з варіативними комбінаціями	174
4.5. Вплив структури алфавіту і ймовірностей на ентропію	176
4.6. Інтеграція процесів шифрування та завадостійкого кодування	177
4.7. Розробка методу формування простору випадкових комбінацій для системи статистичного шифрування	182
4.8. Математичне моделювання криптографічної стійкості статистичного шифрування	194
4.9. Розробка методу інтеграції статистичного шифрування, завадостійкого кодування з декореляцією помилок	199
4.10. Компенсація надлишковості комбінованих методів захисту інформації за допомогою таймерних сигналів	215
Висновки	216

5 Дослідження та обґрунтування вибору параметрів таймерних сигналів в системах захисту інформації на основі розширення

спектра.....	218
5.1. Основні завдання при побудові шумоподібних сигналів з використанням таймерного кодування	218
5.2. Порівняльний аналіз алгоритмів розширення спектра позиційних та таймерних сигналів	220
5.3. Вибір розрядності таймерного кодування	230
5.4. Оцінка числа реалізації за рахунок збільшення значущих моментів модуляції таймерного сигналу	232
5.5. Оцінка впливу базового елементу побудови таймерного сигналу	

на кількісні і якісні показники передавання інформації	234
5.6. Генерування псевдовипадкових послідовностей з підвищеною криптографічної стійкістю	236
5.6.1. Оцінка якості псевдовипадкових послідовностей	236
5.6.2. Тестування та вимоги до псевдовипадкових послідовностей	237
5.6.3. Метод підвищення якісних показників реалізацій генераторів хаосу	240
5.6.4. Синтез послідовностей з підвищеною криптографічною стійкістю	244
5.6.5. Метод формування початкових параметрів для генераторів хаосу	247
Висновки	249
6 Методи формування шумоподібних таймерних сигналів ...	251
6.1. Енергетична прихованість у системах з розширеним спектром.....	251
6.1.1. Умови забезпечення енергетичної прихованості та її роль у захисті від засобів радіоелектронної розвідки	251
6.1.2. Аналіз базових методів розширення спектра	255
6.2. Методи забезпечення структурної прихованості сигналів на основі псевдовипадкових послідовностей та таймерних сигналів	256
6.2.1. Особливості використання псевдовипадкових послідовностей розширення спектра	256
6.2.2. Оцінка впливу таймерних сигналів на структурну прихованість псевдовипадкових послідовностей Уолша	257
6.3. Вибір бази сигналу для розширення спектра таймерних сигналів	263
6.4. Синтез шумоподібних сигналів методом прямого розширення спектра таймерних сигнальних конструкцій	264
6.5. Оцінка структурної прихованості шумоподібних таймерних сигналів	267
6.6. Синтез шумоподібного сигналу методом псевдовипадкового перескоку робочої частоти таймерних сигнальних конструкцій	269
6.7. Метод розширення спектра таймерних сигналів з використанням лінійної частотної модуляції	279

6.8. Метод мультиплексування імпульсів таймерних сигнальних конструкцій	286
6.9. Метод розширення спектра таймерних сигналів на основі хаотичних коливань	291
6.10. Дослідження енергетичної прихованості шумоподібних таймерних сигналів	300
Висновки	306
ВИСНОВКИ.....	308
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	314
Додаток А. Список публікацій здобувача за темою дисертації	333
Додаток Б. Акти впровадження результатів дисертаційної роботи	339

ВСТУП

Актуальність теми. Актуальність теми дослідження зумовлена щораз більшими загрозами інформаційній безпеці, які пов'язані з розвитком засобів несанкціонованого доступу (НСД) та радіоелектронної розвідки (РЕР). Це створює потребу в удосконаленні методів захисту інформації на каналному та фізичному рівнях моделі OSI, особливо в інформаційно-комунікаційних системах (ІКС) із безпроводовим передаванням, які є найбільш вразливими до перехоплення та спотворення даних у середовищі радіоелектронного протиборства.

Законодавство України, зокрема закони «Про інформатизацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про кібербезпеку», «Про захист персональних даних» та «Про електронні довірчі послуги», а також міжнародні стандарти (ISO 7498-2, ISO 10181-1–10181-7, ISO/IEC 27001, ISO/IEC 27002), визначають необхідність забезпечення конфіденційності, цілісності та доступності інформації. Одним із перспективних напрямів захисту переданої інформації є застосування спектральних методів, зокрема розширення спектра вузькосмугового сигналу для підвищення прихованості передачі. Водночас, для ефективного протистояння сучасним загрозам доцільним є використання комплексного підходу до захисту, який передбачає інтеграцію різних методів перетворення сигнальних конструкцій – таких як шифрування, завадостійке кодування та спектральне розширення.

Теоретичні основи використання шумоподібних сигналів (ШПС) для забезпечення прихованості передавання сигнальних конструкцій були закладені провідними науковцями – Г. Найквістом, К. Шенноном, Р. Калманом, Е. Вітербі, І. Джейкобсом, Д. Купером та іншими. Разом із дослідженнями українських учених (В. Литвиненко, М. Захарченко, Б. Радзімовський, В. Гордійчук, А. Зюко, В. Банкет та інших) це створило підґрунтя для розвитку методів спектрального маскування переданої інформації. Однак наявні методи

формування ШПС, зокрема на основі псевдовипадкових послідовностей (ПВП) (наприклад, Уолша, Голда, Касамі), не забезпечують достатнього рівня захисту, оскільки їхня структура є передбачуваною і піддається відновленню за допомогою кореляційного аналізу або статистичного спектрального моніторингу.

Перспективним підходом до забезпечення цілісності інформації є використання таких методів завадостійкого кодування, які можуть гарантувати як достовірність передавання, так і сприяти підвищенню захисту від НСД в складі комбінованих систем захисту. У цьому контексті доцільним є дослідження властивостей непозиційних сигналів, зокрема таймерних сигнальних конструкцій (ТСК), які були запропоновані М. Захарченком. Використання ТСК у поєднанні з розрядно-цифровим кодуванням (РЦК) дозволяє не лише здійснювати контроль достовірності передавання, але й розробляти алгоритми захисту інформації від НСД. Подальший розвиток технологій захисту інформації в умовах впливу завад і НСД можливий завдяки інтеграції різних методів перетворення даних: стохастичного шифрування, завадостійкого кодування та алгоритмів зменшення групування помилок у кодових блоках. Важливим напрямом дослідження для підвищення прихованості є розробка методів формування шумоподібних таймерних сигналів. Складність реалізації таких методів пояснюється непозиційністю імпульсних складових ТСК, для яких непридатні класичні підходи до спектрального розширення, розроблені для позиційних кодів. Розвиток теорії таймерного кодування із застосуванням методів розширення спектра сигналів та хаотичних коливань забезпечить ефективніше функціонування інформаційно-комунікаційних систем в умовах навмисних завад і підвищить рівень захисту переданих повідомлень від перехоплення. Водночас постійне вдосконалення засобів радіотехнічної розвідки обумовлює необхідність розробки нових підходів до ускладнення спектральної структури сигналів у процесі передавання.

Актуальність теми дисертаційного дослідження полягає в потребі

створення та аналізу нових методів підвищення захищеності ІКС шляхом інтеграції методів кодування, шифрування та розширення спектра. Реалізація таких підходів сприятиме формуванню ефективних механізмів протидії сучасним загрозам інформаційній безпеці та забезпечить високий рівень конфіденційності, цілісності й доступності інформації в умовах дії радіоелектронних загроз.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота підготовлена у відповідності до основних положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Стратегії кібербезпеки України. Тема дослідження пов'язана з науковими напрямами, сформульованими в п. 1.2.9 та п. 1.2.9.5 – теорія та комп'ютерні технології інформаційної безпеки "Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук національної академії наук України на 2024–2028 роки", затверджених постановою Президії НАН України від 10.01.2024 №8, а також з напрямами, які корелюють із науково-технічними завданнями Постанови Кабінету Міністрів України № 942 від 7.09.2011 р. із змінами, внесеними постановою КМ № 463 від 9.05.2023 р. «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року» (Розділ «Інформаційні та комунікаційні технології», підрозділ «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби РЕБ для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека»). Тема роботи пов'язана з такими пріоритетними напрямами наукових досліджень у ДУІТЗ, як: теоретичні дослідження та розробка методів захисту інформації від НСД в ІКС і мережах; методи захисту передаваної інформації з використанням розширення спектра непозиційних сигналів; розробка методів захисту інформації на основі комбінованих методів перетворення даних з використанням стохастичного шифрування, завадостійкого кодування та хаотичних сигнальних конструкцій.

Результати досліджень дисертаційної роботи увійшли до складу науково-технічних звітів з держбюджетних науково-дослідних робіт за темами: «Підвищення ефективності використання нестаціонарних каналів з базою $\Delta Ft_0=1$ » (державний реєстраційний номер 0111U005680); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0111U007643); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0112U006815); «Підвищення ефективності використання нестаціонарних каналів з базою $\Delta Ft_0=1$ » (державний реєстраційний номер 0112U006814); «Підвищення ефективності використання нестаціонарних каналів з базою $\Delta Ft_0=1$ » (державний реєстраційний номер 0113U004750); «Ефективність систем інформаційної безпеки» (державний реєстраційний номер 0113U004749).

Мета та задачі дослідження.

Метою дисертаційної роботи є розв'язання науково-технічної проблеми підвищення захищеності передаваної інформації в інформаційно-комунікаційних системах шляхом розробки моделей та методів параметричного перетворення сигнально-кодових конструкцій, що забезпечують підвищену завадостійкість, прихованість та стійкість до несанкціонованого доступу.

Поставлена мета зумовила необхідність розв'язання таких завдань:

1) Розробити узагальнену модель захисту інформації на основі показників завадозахищеності (завадостійкості та прихованості) ІКС з урахуванням енергетичних, частотних та інформаційних ресурсів каналу зв'язку та граничних умов їх функціонування. На основі цієї моделі оцінити показники захисту інформації від НСД за критеріями енергетичної, структурної та інформаційної прихованості. Провести аналіз ефективності використання позиційних і непозиційних сигналів для формування шумоподібних сигнально-кодових конструкцій у комбінованих методах захисту інформації на основі інтеграції стохастичного шифрування, завадостійкого та таймерного кодування.

2) Оцінити ефективність сумісного використання таймерних і позиційних кодів для адаптації параметрів передавання сигнально-кодових конструкцій в ІКС, що функціонують в умовах нестаціонарного каналу зв'язку.

3) Проаналізувати ефективність застосування непозиційних ТСК для підвищення структурної прихованості та завадостійкості шляхом варіювання параметрів таймерного кодування. Виявити закономірності між рівнем структурної прихованості та завадостійкості на основі вибору оптимального значення параметра Δ як базового елемента формування ТСК, а також оцінити здатність таймерного кодування до виявлення та виправлення спотворень у сигнально-кодових конструкціях.

4) Розробити багаторівневу систему захисту інформації, яка забезпечує синергетичне поєднання статистичного шифрування, завадостійкого, таймерного кодування та декореляції помилок. Оцінити ефективність використання таймерних сигналів для компенсації надлишкових елементів, які виникають у процесі статистичного шифрування та завадостійкого кодування.

5) Провести аналіз впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Запропонувати критерії вибору параметрів ТСК з урахуванням складності їх реалізації, а також вимог до забезпечення прихованості та завадостійкості.

6) Дослідити та оцінити методи синтезу шумоподібних сигналів на основі ТСК з використанням різних підходів до спектрального розширення. Розробити умови забезпечення енергетичної прихованості для обраних методів. Запропонувати алгоритми розширення спектра із застосуванням ТСК та сформулювати методику обчислення показників структурної прихованості шумоподібних сигналів.

Об'єктом дослідження є процеси формування та інтеграції методів захисту інформації в сигнально-кодових конструкціях для забезпечення прихованості під час передавання в інформаційно-комунікаційних системах.

Предметом дослідження є методи та алгоритми параметричного перетворення сигнально-кодових конструкцій, спрямовані на підвищення прихованості та завадостійкості передавання інформації в умовах радіоелектронного конфлікту.

Методи дослідження. У дисертаційній роботі використано сукупність

методів і прийомів, заснованих на принципах системного аналізу, формалізації та моделювання. Зокрема, дослідження базуються на методах, що ґрунтуються на теоріях прихованості, криптографії, радіоелектронних систем і комплексів, теорії ймовірностей та моделювання складних систем. Для перевірки гіпотез і оцінювання ефективності запропонованих рішень застосовано математичне та імітаційне моделювання.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає у вирішенні важливої науково-прикладної проблеми підвищення захищеності ІКС шляхом розробки нового теоретичного підходу до інтеграції методів параметричного перетворення сигнально-кодових конструкцій. Запропоновано концепцію сумісного використання непозиційних таймерних сигналів, методів розширення спектра, стохастичного шифрування, завадостійкого кодування та алгоритмів декореляції помилок з метою зниження спотворення кодових блоків.

Наукова новизна одержаних результатів полягає в наступному:

1) Уперше запропоновано модель оцінювання захищеності передачі інформації на основі обсягу сигналу, яка дозволяє наочно оцінювати відповідність характеристик сигналу можливостям каналу та приймати рішення щодо методів узгодження або параметричного перетворення сигналу. Це дозволяє здійснювати оцінку рівня захищеності за критеріями енергетичної, структурної та інформаційної прихованості відповідно до умов функціонування ІКС.

Уперше запропоновано узагальнену модель вдосконалення методів прихованого передавання інформації, яка дозволяє здійснювати порівняльний аналіз методів захисту за критеріями прихованості та завадостійкості.

2) Уперше запропоновано метод взаємного обміну якості та швидкості передавання інформації шляхом комбінованого застосування таймерних і позиційних кодів у нестаціонарних каналах зв'язку, що дозволяє підвищити захищеність та ефективність систем зв'язку в умовах радіоелектронного конфлікту.

3) Уперше запропоновано метод одночасного захисту інформації від НСД та випадкових завад у каналі зв'язку, що дозволило встановити залежність рівня структурної прихованості ТСК та завадостійкості від мінімальної кодової відстані дозволених комбінацій, які визначаються як за рівнянням якості, так і шляхом повного перебору всіх можливих сигнальних конструкцій.

4) Уперше розроблено багаторівневу модель захисту інформації, яка забезпечує синергетичне поєднання статистичного шифрування, завадостійкого та таймерного кодування, а також процедури декореляції помилок. Такий підхід дозволяє одночасно на кожному рівні моделі підвищити криптостійкість, завадостійкість та захист від НСД. Обґрунтовано доцільність використання таймерних сигналів для компенсації надлишкових елементів, які виникають у процесі статистичного шифрування та завадостійкого кодування.

5) Уперше встановлено закономірності впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Розроблено критерії вибору параметрів, які забезпечують баланс між складністю реалізації, пропускнуою здатністю та прихованістю передавання даних. Виявлено протиріччя між прагненням до підвищення структурної прихованості шляхом збільшення параметра s та необхідністю його обмеження до оптимального значення $S_{\text{опт}}$, що визначається співвідношенням сигнал/шум у каналі.

6) Розвинуто теорію систем зв'язку з шумоподібними сигналами шляхом створення нових методів розширення спектра непозиційних сигналів на основі псевдовипадкового перескоку робочої частоти (ППРЧ), прямого розширення спектра псевдовипадковими послідовностями (ПРС-ПВП) та лінійної частотної модуляції (ЛЧМ) з визначенням оптимальних параметрів таймерних сигналів. Запропоновано умови забезпечення енергетичної прихованості для методів розширення спектра на основі критеріїв частотної та енергетичної ефективності використання каналу.

Практичне значення одержаних результатів.

Дисертаційним дослідженням розроблено методи параметричного

перетворення сигнально-кодкових конструкцій для забезпечення захисту інформації на основі прихованості сигналів та достовірного аналізу й кількісного оцінювання рівня захищеності інформаційно-комунікаційних систем.

Найбільш важливими практичними результатами дисертаційної роботи є:

- Розроблено алгоритм адаптивного обміну між завадостійкістю та швидкістю передавання залежно від стану нестационарного каналу зв'язку. Встановлено, що сумісне використання ТСК і РЦК дозволяє підвищити завадостійкість в 1,59 рази при зростанні відносної швидкості передавання від $R_{\text{РЦК}} = 0,55$ до $R_{\text{РЦК-ТСК}} = 1,05$, що водночас забезпечує зменшення часу передавання заданого обсягу інформації у два рази.

- Розроблено алгоритм підвищення структурної прихованості та завадостійкості шляхом формування ТСК із варіативним використанням параметрів n , i та s , що забезпечує збільшення кількості можливих реалізацій у 10 і більше разів порівняно з позиційними кодами. Встановлено залежність зменшення кількості реалізацій ТСК приблизно у 2, 7, 12 та 22 рази при збільшенні мінімальної кодової відстані $d_0 = 2, 3, 4, 5$ відповідно. Виявлено зворотну залежність між показниками структурної прихованості та завадостійкості, що зумовлена зменшенням значення базового елемента побудови таймерного сигналу Δ .

- Розроблено багаторівневу модель системи захисту інформації на основі інтеграції стохастичного шифрування із завадостійким кодуванням, декореляцією помилок і таймерним кодуванням, у які додатково вбудовані механізми захисту від НСД. У межах реалізації стохастичного шифрування запропоновано алгоритм формування шифрограми шляхом добору випадкових кодкових комбінацій з урахуванням імовірності появи символів у відкритому тексті. Показано, що при довжині випадкових комбінацій $n=9, 10, \dots, 17$ досягається зменшення дисперсії розподілу ймовірностей символів (D_{xy}) до нуля, зокрема у 28, 47, $\dots$, 57269 разів, залежно від довжини комбінації. Це

унеможливилося ефективне застосування частотного криптоаналізу при перехопленні повідомлень. Для компенсації надлишковості шифрограми, що виникає внаслідок стохастичного шифрування та блокового кодування, запропоновано використовувати таймерні сигнали, які дозволяють оптимізувати тривалість передавання без втрати стійкості до атак.

– На основі встановлених закономірностей розроблено методику вибору параметрів таймерних сигналів для формування шумоподібних сигналів. Проведено аналіз впливу фіксованої кількості значущих моментів відновлення (ЗММ) у ТСК, який показав, що максимальна кількість реалізацій досягається при значенні параметра i , зазвичай на 2–4 одиниці меншим за m . Визначено, що зі зростанням інтервалу побудови сигналів ($m = 6, 7, \dots, 19$) структурна прихованість зростає (для прикладу при $s = 7, i = 4$ вона становить від 12 до 22 умовних одиниць). Показано можливість подвоєння структурної прихованості шляхом використання комбінацій з різними значеннями ЗММ i . Обґрунтовано вибір оптимального значення параметра s_o , який залежить від співвідношення сигнал/шум h у каналі й при якому забезпечується максимальна пропускна здатність $C_{\text{тск}}$ при одночасному досягненні заданого рівня прихованості. Встановлено, що надмірне зменшення часового інтервалу Δ при $s > s_{\text{опт}}$ призводить до збільшення показника втрат H_3 , який характеризує рівень спотворених сигнальних конструкцій. Виявлено протиріччя між прагненням до підвищення структурної прихованості через збільшення s та необхідністю його обмеження до $s \leq s_{\text{опт}}$ при фіксованому m і h .

– Розроблено нові алгоритми розширення спектра для таймерних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ), які враховують структуру непозиційних сигнальних конструкцій. На відміну від відомих методів для позиційних кодів, запропоновані алгоритми забезпечують: розширення спектра на інтервалі всієї комбінації таймерних сигналів, що передбачає визначення кількості імпульсів розширення $N_{\text{тск}} = B_{t_0} \times m$ з урахуванням бази елемента Найквіста B_{t_0} ; вибір параметрів (m, s, i) з урахуванням співвідношення сигнал/шум у каналі; формування широкосмугових сигналів зі спектральними характеристиками,

придатними для застосування в реальних ІКС з підвищеними вимогами до завадостійкості та прихованості. Запропоновано комбінований метод розширення спектра таймерних сигналів на основі поєднання ПРС-ПВП та ППРЧ. Використання двох баз розширення спектра таймерного сигналу дозволяє істотно підвищити структурну прихованість сигнально-кодових конструкцій, рівень якої за криптостійкістю є співставним з протоколами шифрування DES та AES.

– Розроблено нові алгоритми кореляційного прийому широкосмугових таймерних сигналів (для ПРС-ПВП та ЛЧМ), які враховують структуру побудови непозиційних сигналів. Вони забезпечують прийняття рішень щодо значущих моментів відновлення фронтів в межах усієї сигнальної конструкції та передбачають використання кореляційного приймача з пристроєм визначення екстремумів напруги на виході інтегратора.

– Розроблено умови забезпечення енергетичної прихованості для методів розширення спектра – ППРЧ, ПРС-ПВП та ЛЧМ. Ці умови базуються на трьох критеріях: база сигналу $B = \Delta f T \gg 1$; частотна ефективність $\gamma = R / \Delta f_{\text{еф}}$; енергетична ефективність і $\beta = R / h_0^2$. Аналіз показав, що методи ППРЧ та ЛЧМ задовольняють лише першу та другу умови, тоді як метод ПРС-ПВП – усі три, що свідчить про його перевагу з пог енергетичної прихованості. З урахуванням особливостей непозиційного характеру ТСК запропоновано принцип розширення спектра на інтервалі побудови сигнальної конструкції T_c , що забезпечує підвищену структурну прихованість у порівнянні з позиційними кодами (РЦК). Проведено кількісний аналіз впливу параметрів ТСК на структурну прихованість. Наприклад, при $m = 8$, $s = 5$, $i = 3$, базова структурна прихованість дорівнює $S_{\text{ТСК}} = 12$ дв.вим. Розширення спектра методом ПРС-ПВП із базою $B_{t_0} = 8$ і $N_{\text{ПВП}} = 64$, а також застосування модуляції ФМ-2, дозволяє збільшити прихованість до $S_{\text{ТСК ПВП}} = 77$ дв.вим. Подальше збільшення бази до $B_{t_0} = 16$ і $N_{\text{ПВП}} = 128$ дозволяє досягти значення $S_{\text{ТСК ПВП}} = 141$ дв.вим. Отже, структура ПВП після розширення спектра кожної

ТСК стає унікальною, що значно ускладнює аналіз та ідентифікацію сигнальних конструкцій у каналі зв'язку.

Одержані в роботі наукові і практичні результати знайшли впровадження в діяльності, що підтверджено відповідними актами КП «Обласний інформаційно-аналітичний центр» Одеської обласної ради, ПП «АРДО», а також у навчальному процесі кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку в процесі викладання дисциплін для підготовки бакалаврів та магістрів за напрямом 125 «Кібербезпека та захист інформації».

Особистий внесок здобувача. Усі результати наукових, теоретичних і практичних досліджень, які викладено в дисертації, отримано автором самостійно.

В [1, 7] автору належить розробка алгоритму розширення спектра таймерних сигналів, який полягає у використанні двох несучих частот ЛЧМ для позитивних та негативних імпульсів сигнальних конструкцій. В [2, 6, 8] автору належать спільні зі співавторами розробка та аналіз ефективності комбінованих методів захисту даних за допомогою стохастичного шифрування та таймерного кодування. В [3, 26, 29] автору належить аналіз ефективності застосування гомоморфних криптосистем у рекомендаційних системах веб-сервісів. В [4, 30] автору належить розробка алгоритму двійкової псевдовипадкової послідовності з підвищеною криптографічною стійкістю на основі програмних генераторів хаосу. В [5, 37, 42] автору належить статистичні дослідження генераторів хаосу та обґрунтування застосування їх у криптографічних системах. В [9, 13, 36, 39, 40] автору належать спільні із співавторами алгоритми розширення спектра таймерних сигналів на основі ППРЧ та формулювання висновків. В [10] автором надана оцінка енергетичної прихованості функціонування радіотехнічних систем на основі прямого розширення спектра таймерних сигналів. В [11, 12, 28] автору належать розрахунок енергетичної та структурної прихованості таймерних сигналів з урахуванням забезпечення заданої достовірності передавання даних. В [14] автору належать спільні із співавторами розробка системи оцінок для

порівняльного аналізу методів підвищення енергетичної та структурної прихованості шумоподібних сигналів з урахуванням зміни частотної та енергетичної ефективності каналу. В [15] автору належать спільні із співавторами аналіз ефективності використання двосимвольних ансамблів у симплексних системах на базі коригувальних ТСК. В [16, 38, 41] автору належать спільні зі співавторами розробки алгоритмів мультиплексування імпульсів таймерних сигналів. В [16] автору належать розрахунки інформаційних параметрів кодів Сліп'яна з компенсацією надлишковості таймерними сигналами. В [17, 27] автору належать спільні із співавторами розробка та аналіз методів підвищення прихованості передавання на основі розширення спектра непозиційних ТСК з використанням технологій FHSS і DSSS, а також розглядаються особливості використання кореляційного прийому шумоподібних таймерних сигналів. В [18] автору належать розрахунки та формулювання висновків, щодо ідентичності об'єктів інформаційної мережі як елементу моделі кібербезпеки. В [19] автору належать спільні із співавторами розробка методу підвищення прихованості сигнальних конструкцій передавання на основі сумісного використання хаотичних та таймерних сигналів. В [20] автору належить розрахунок завадостійкості передавання даних при j -кратному повторенні надлишкових ТСК. В [21] автору належать спільні із співавторами аналіз та розрахунок завадостійкості в умовах впливу корельованих завад та аналіз пропускну здатності безперервного каналу зв'язку. В [22] автору належить аналіз завадостійкості і розрахунок компенсації надлишковості в блокових коректуючих кодах за рахунок ТСК та формулювання висновків. В [23] автору належать спільні із співавторами розробка моделі спільного використання системи виявлення й обробки атак із системою постійного аудиту інформаційної безпеки. В [24] автору належить розробка адаптивного алгоритму синтезу шумоподібних сигналів шляхом зміни параметрів ТСК у залежності від поточного стану каналу зв'язку. В [25] автором запропоновано систему оцінок захищеності методів захисту передаваної інформації в умовах РЕБ. В [28] автором запропонована методика підвищення структурної прихованості

сигнальних конструкцій на основі сумісного використання ТСК і методів маніпуляції. В [31, 36, 43] автору належать спільні із співавторами розробка алгоритму підвищення прихованості передавання даних для системи з кодовим розділенням каналів на основі послідовностей динамічного хаосу. В [32] автору належать спільні із співавторами розробка методів підвищення структурної прихованості на основі шумоподібних таймерних сигналів. В [33] автором запропонована методика підвищення структурної прихованості даних на основі випадкового таймерного кодування. В [34] автору належать спільні із співавторами методика розробки комбінованого методу захисту інформації на основі сумісного використання завадостійкого кодування, таймерних сигналів і хаотичних реалізацій. В [35] автором надано аналіз умови забезпечення захищеності систем зв'язку спеціального призначення. В [44] автору належить аналіз доцільності застосування зворотного зв'язку в системах передачі даних та формування висновків дослідження.

Апробація результатів дисертації. Основні наукові результати дисертаційної роботи доповідались на 21-му міжнародному та всеукраїнському симпозіумі, науково-практичній та науково-технічній конференціях [24–44] у таких містах: Київ, Одеса, Славськ, Львів, Чернівці, Черкаси, Буча.

Публікації. За матеріалами дисертаційної роботи опубліковано 44 наукових праць, зокрема: 1 монографія [1], 22 статті [2–23], з яких 20 статей у фахових наукових журналах, що входять до переліку МОН України [2–4, 7–23], зокрема 1 стаття [2] в журналі, який цитується в наукометричній базі даних Scopus та 1 стаття [8] – у наукометричній базі даних Web of Science. Дві статті [5, 6] опубліковано в іноземних фахових виданнях, які цитуються в наукометричній базі даних Scopus. Апробація досліджень дисертації: 21 публікація опублікована в матеріалах міжнародних та всеукраїнських симпозіумів, науково-практичних та науково-технічних конференцій [24–44], з яких 5 наукових праць [24, 27, 27, 28, 34] – у виданнях, які цитуються у наукометричній базі даних Scopus. Загальна кількість наукових праць у виданнях, які цитуються у наукометричних базах даних Scopus та Web of

Science складає 9, з яких – 4 статті та 5 тез до конференцій. Крім зазначених робіт, складено 6 звітів з НДР за спеціальною тематикою.

Структура й обсяг роботи. Робота складається зі вступу, шести розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 340 сторінок, із них 291 – основного тексту з 65 рисунками та 36 таблицями, список використаних джерел нараховує 154 найменувань на 19 сторінках, 8 сторінок додатків.

1 СТАН ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В СУЧАСНИХ УМОВАХ. ВИБІР НАПРЯМКІВ ДОСЛІДЖЕНЬ

У розділі проведено огляд і аналіз сучасного стану проблеми забезпечення захищеності інформаційно-комунікаційних систем в умовах активного використання засобів радіоелектронної боротьби. Досліджено наукові підходи до оцінювання завадостійкості, енергетичної та структурної прихованості, а також криптографічного захисту. Обґрунтовано доцільність побудови узагальненої моделі захисту інформації, яка враховує обмеження каналного ресурсу та граничні умови функціонування. Розкрито актуальність реалізації багаторівневого захисту в межах моделі OSI з акцентом на фізичному та каналному рівнях. Запропоновано модель системи оцінок захищеності сигналів, що дозволяє порівнювати ефективність різних сигнально-кодових конструкцій з урахуванням взаємозв'язку між показниками завадозахищеності та прихованості.

1.1. Теоретичне обґрунтування захисту інформації на основі показників прихованості та завадостійкості

Одним із підходів до захисту конфіденційної інформації від несанкціонованого доступу в каналах зв'язку є застосування методів передавання сигналів, які забезпечують високий рівень завадозахищеності [1-3].

Завадозахищеність є комплексною характеристикою [1, 2], що відображає здатність інформаційно-комунікаційної системи забезпечувати як захист даних від несанкціонованого доступу [3-6] шляхом перетворення інформації у сигнальні конструкції з властивостями прихованості (енергетичної, структурної та інформаційної та інші), так і гарантувати достовірність та цілісність

передавання повідомлень в умовах дії завад. Високий рівень завадозахищеності дозволяє зберігати працездатність системи навіть за умов активного впливу, зокрема у разі спроб перехоплення, спотворення або придушення сигналу.

Отже, завадозахищеність є інтегральним показником стійкості системи передавання інформації до впливу деструктивних факторів, зокрема навмисних радіоелектронних завад [7-9], спроб перехоплення або спотворення сигналу. Цей показник поєднує як здатність зберігати достовірність та цілісність переданих повідомлень, так і ефективність захисту інформації від несанкціонованого доступу шляхом застосування сигнально-кодових конструкцій із властивостями прихованості [10]. Залежно від характеру загроз, виділяють три основні складові прихованості сигналів, що водночас виступають окремими характеристиками завадозахищеності [1, 2]:

1) енергетична прихованість відображає здатність системи протидіяти заходам, спрямованим на виявлення самого факту передавання сигналу. Досягається шляхом зниження енергетичної помітності сигналу, наприклад, використанням малопотужних, шумоподібних сигналів, які наближаються або менше рівня фонових завад у каналі зв'язку;

2) структурна прихованість характеризує здатність сигналу залишатися нерозпізнаним навіть у разі його виявлення. Це означає ускладнення аналізу форми сигналу, його параметрів (частоти, фази, амплітуди, тривалості тощо) та віднесення до відомих зразків. Зазвичай досягається за рахунок хаотичних або квазівипадкових змін структури сигналу, а також використання нестандартних або адаптивних схем модуляції;

3) інформаційна прихованість визначає стійкість системи до спроб розкриття вмісту переданих повідомлень, навіть якщо форма сигналу була частково або повністю відновлена. Забезпечується за допомогою криптографічного перетворення, використання псевдовипадкових послідовностей, методів потокового шифрування, кодів із секретними параметрами тощо.

У сукупності ці показники визначають здатність системи ефективно функціонувати в умовах радіоелектронної протидії [10-14] та спротиву зовнішньому втручанню [15-16], що є критично важливим для забезпечення надійного й захищеного зв'язку в сучасних умовах.

Енергетична прихованість [1, 2] реалізується за рахунок зменшення ймовірності виявлення факту передавання сигналу в каналі зв'язку. Це досягається шляхом мінімізації енергетичної помітності сигналу на фоні шумів або природних завад, тобто створенням таких умов, за яких сигнал стає "невидимим" для засобів радіоконтролю противника. Одним із ключових параметрів, що визначають енергетичну прихованість сигналу, є спектральна густина потужності сигналу на частоті f :

$$S_s(f) = \frac{P_s}{B_s}, \quad (1.1)$$

де P_s – середня потужність сигналу, B_s – ширина спектра сигналу.

Вочевидь, що для підвищення енергетичної прихованості необхідно зменшити $S_s(f)$ таким чином, щоб вона була нижчою або порівнянною з спектральною густиною шуму $S_n(f)$, тобто:

$$S_s(f) \leq S_n(f). \quad (1.2)$$

У таких умовах відношення сигнал/шум (SNR) у приймачі зловмисника противника буде меншим за порогове значення виявлення:

$$\text{SNR}_{\text{адв}} = \frac{P_s}{P_n}, \quad (1.3)$$

де P_n – потужність шуму в смузі пропускання приймача, $\text{SNR}_{\text{адв}}$ – порогове значення відношення сигнал/шум, за якого ще можливе виявлення сигналу засобами радіорозвідки.

З урахуванням використання сигналів з розширеним спектром [17-19] (наприклад, у системах DSSS або FHSS), ширина спектра F_s значно збільшується, що призводить до зменшення $S_s(f)$, згідно з формулою (1.1). У результаті отримуємо наступне:

$$\frac{P_s}{\Delta F_s} \leq S_n(f), \quad (1.4)$$

тобто сигнал маскується фоновим шумом і становиться практично його виявити засобами радіоелектронної розвідки [20]. На рис. 1.1 представлена залежність спектральної густини потужності сигналу $S_s(f)$ від ширини спектра ΔF_s .

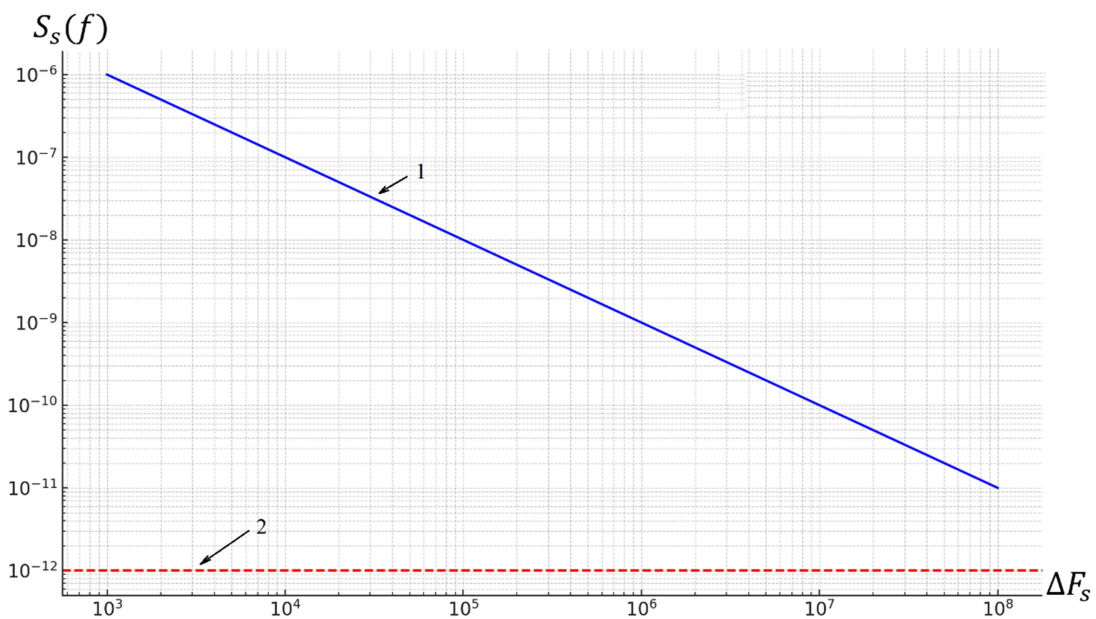


Рисунок 1.1 – Залежності спектральної густини потужності сигналу $S_s(f)$ від ширини спектра ΔF_s

Залежність під номером 1 рис. 1.1 демонструє, як при зростанні ширини спектра зменшується енергетична прихованість сигналу, тобто сигнал «розмазується» по широкому діапазону частот. Інша залежність під номером 2 демонструє рівень фонові спектральної густини шуму $S_n(f)$. Як бачимо, сигнал стає енергетично прихованим, оскільки його складові не виділяються з

шумового фону. Це ключовий принцип підвищення енергетичної прихованості за рахунок розширення спектра сигналу. Можна визначити основні підходи до реалізації енергетичної прихованості, в яких використовують різні методи розширення спектра початкового вузько смугового сигналу [21-23]:

- 1) пряме розширення спектра (ПРС – DSSS – Direct Sequence Spread Spectrum);
- 2) псевдовипадковий перескок робочої частот (ППРЧ – FHSS – Frequency Hopping Spectrum Spreading);
- 3) лінійна частотна модуляція (ЛЧМ – LFM – Linear Frequency Modulation);
- 4) комбінований спосіб розширення спектра на основі ПРС та ППРЧ.

Критично важливим параметром широкосмугового сигналу є база сигналу, яка служить для оцінки ефективності систем з розширеним спектром. Як правило база визначає співвідношення між шириною спектра сигналу та його тривалістю:

$$B = \tau \Delta f \gg 1, \quad (1.5)$$

де T – тривалість сигналу, Δf – ширина спектра сигналу.

Слід відзначити [24, 25], що збільшення бази сигналу сприяє значному підвищенню енергетичної та структурної прихованості широкосмугових сигналів, знижуючи їх спектральну щільність потужності та ускладнюючи виявлення і класифікацію противником. Велике значення бази забезпечує кращу завадостійкість, високу часову та частотну роздільну здатність, а також підвищує ефективність засобів маскування сигналу в умовах радіоелектронної боротьби. Однак, з іншого боку, практична реалізація сигналів із великою базою стикається з низкою технічних обмежень, таких як: вимоги до широкосмугових підсилювачів та антен; необхідність забезпечення більших вимог до систем циклової та тактової синхронізації; більшу складність генерації та обробки височастотних псевдовипадкових послідовностей;

обмеження з боку спектрального ресурсу. Отже, при проєктуванні систем із великою базою сигналу необхідно враховувати компроміс між покращеними характеристиками прихованості та технічними можливостями апаратної реалізації.

1.2. Захист інформації на основі методів розширення спектра

1.2.1. Метод прямого розширення спектра сигналу

Пряме розширення спектра [21, 25-27] забезпечує спектральне маскування, при якому вузькосмуговий інформаційний сигнал $x(t_0)$ множиться на бінарну псевдовипадкову послідовність (ПВП) $c(\tau)$, яка має значно вищу швидкість, ніж інформаційна. В результаті отримаємо наступну широкосмуговий сигнал (рис.1.2):

$$c_{шс}(\tau) = x(t_0) \times c(\tau) \quad (1.6)$$

Характерним при цьому є те, що послідовність розширення спектра $c(\tau)$ має значно вищу частоту, тобто:

$$c(\tau) \gg x(t_0). \quad (1.7)$$

Ключовою характеристикою методу ПРС є фактор розширення спектра:

$$G_p = \frac{c(\tau)}{x(t_0)} = N_q, \quad (1.8)$$

де N_q – кількість ПВП (чипів), призначених для розширення одного інформаційного біту. Значення N_q показує, наскільки збільшується ширина спектра. Якщо вхідний вузькосмуговий сигнал мав смугу $\Delta f_{вс}$, то після

множення на високочастотний ПВП розширення смуга збільшується приблизно до:

$$\Delta f_{\text{шс}} \approx \Delta f_{\text{ПВП}}, \quad (1.9)$$

тобто:

$$\Delta f_{\text{шс-прс}} \approx \Delta f_{\text{вс}} \times N_{\text{ч}}, \quad (1.10)$$

де $\Delta f_{\text{ПВП}}$ – смуга частот ПВП розширення спектра.

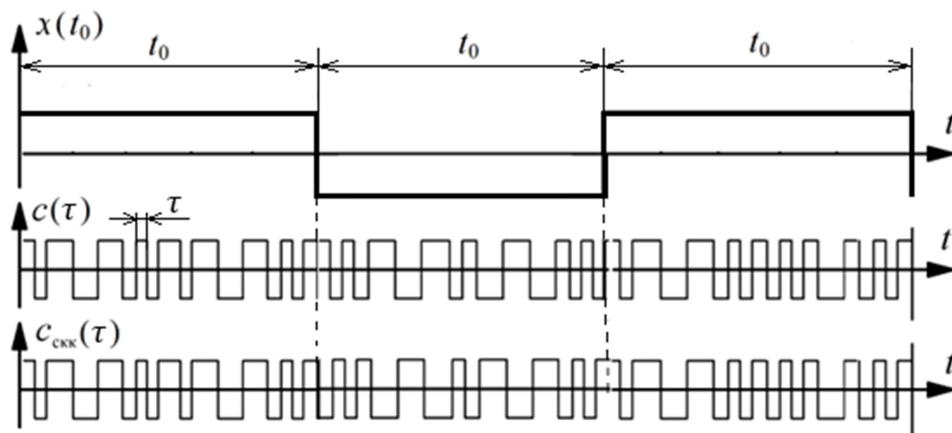


Рисунок 1.2 – Пряме розширення спектра інформаційного сигналу ПВП

Отже, алгоритм (1.6) дозволяє значно розширити спектр сигналу і зменшити його спектральну щільність потужності [26-27]. При цьому ускладняється виявлення засобами РЕР [28-30] сеанси зв'язку та робить сигнал більш стійким до завад. Для порівняння на рис. 1.3 представлено спектр вузькосмугового інформаційного сигналу $S_{\text{с вуз}}(f)$ та спектр сигналу $S_{\text{с роз}}(f)$ після застосування прямого розширення за допомогою ПВП.

1.2.2. Метод розширення спектра на основі псевдовипадкового перескоку робочої частоти

Метод формування широкосмугового сигналу на основі ППРЧ [21] використовує частоту несущого коливання, яка змінюється стрибкоподібно

згідно деякої псевдовипадкової послідовності. Сигнал передавання в цьому випадку можна представити як:

$$s(t) = A \cdot m(t) \cdot \cos(2\pi f_i(t)t + \varphi, \quad t \in [t_i, t_{i+1}] \quad (1.11)$$

де A – амплітуда сигналу, $f_i \in \{t_1, t_2, \dots, t_N\}$ – набір частот, між якими здійснюється перестрибування, φ – початкова фаза, яка може бути змінною).

Псевдовипадкова послідовність зміни несучих частот задається наступним чином:

$$f_i(t) = f_{min} + \Delta f_{кр} \cdot h_i(t), \quad (1.12)$$

де $\Delta f_{кр}$ – крок між несущими частотами, $h_i(t) \in \{0, 1, \dots, N - 1\}$ – значення псевдовипадкової послідовності на i -й ітерації.

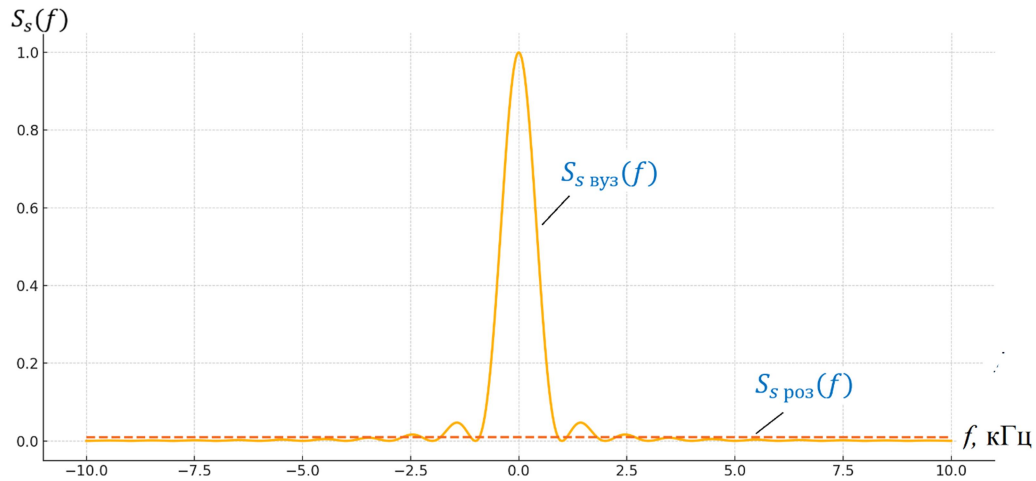


Рисунок 1.3 – Спектр вузькосмугового інформаційного сигналу $S_{s \text{ вуз}}(f)$ та спектр сигналу $S_{s \text{ роз}}(f)$ після застосування прямого розширення

Ширина всього спектра передачі методом ППРЧ визначається як:

$$\Delta f_{шс-ппрч} \approx \Delta f_{кр} \times N_{ппрч}, \quad (1.13)$$

де $N_{\text{ппрч}}$ – кількість частотних каналів.

Тривалість одного стрибка методом ППРЧ визначається як:

$$T_d = \frac{1}{R_d}, \quad (1.14)$$

де: R_d – частота змін частотного каналу.

Розширення спектра інформаційного сигналу методом ППРЧ представлено на рис. 1.4. Тривалий час вважалося, що метод ППРЧ [32] забезпечує достатньо високий рівень енергетичної прихованості переданого сигналу, ускладнюючи його виявлення засобами радіоелектронної розвідки. Це пояснювалося широким розподілом енергії сигналу в частотному діапазоні, що знижувало його спектральну щільність на кожній окремій частоті. Однак стрімкий розвиток сучасної елементної бази, зокрема поява високопродуктивних мікроконтролерів і програмно-конфігурованих SDR-приймачів [32], призвів до створення високошвидкісних сканерів спектра. Завдяки цьому засоби РЕР тепер здатні в реальному часі проводити детектування, аналіз і фіксацію ППРЧ-сигналів навіть за умов їхньої низької енергетичної помітності.

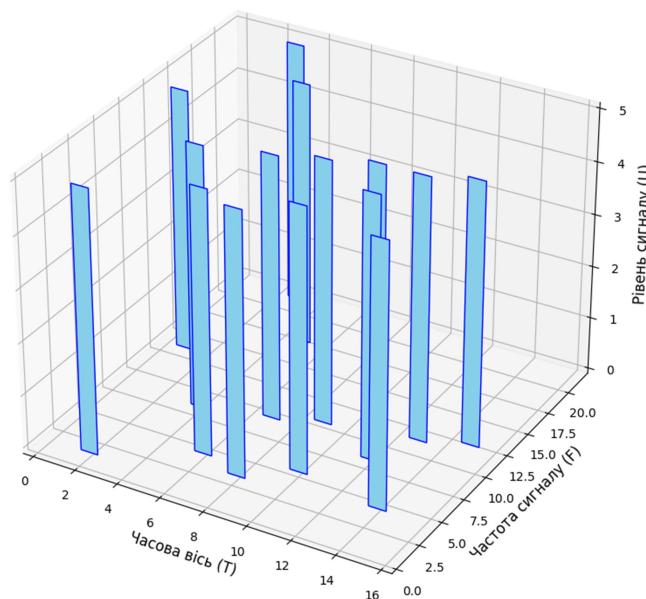


Рисунок 1.4 – Розширення спектра інформаційного сигналу методом ППРЧ

Один із критичних факторів методу ППРЧ – це інтервал перебування сигналу на одній частоті. На практиці цей час є достатньо тривалим (у межах мілісекунд), щоб SDR-приймач встиг провести дискретизацію сигналу, визначити частоту і навіть зафіксувати момент перестрибування. З одного боку, зменшення часу передавання на одній частоті (швидка ППРЧ) дійсно дозволяє підвищити рівень енергетичної прихованості, оскільки сигнал стає більш динамічним та менш передбачуваним у частотному домені. Але з іншого боку, це знижує енергетичний потенціал сигналу, оскільки менше енергії встигає накопичитись у вузькій смузі за короткий час. Це прямо впливає на дальність і надійність приймання: сигнал стає менш стійким до шумів і завад, особливо при великій відстані між передавачем і приймачем.

Зробимо оцінку ефективності методу ППРЧ з урахуванням зменшення часу передавання сигналу T_d на одній несущій частоті. Енергія сигналу, що передається за час:

$$T_t = P_t \times T_d. \quad (1.15)$$

Прийнята енергія сигналу протягом інтервалу часу T_t в системі ППРЧ визначається за формулою Фріса:

$$P_r = \frac{P_t \cdot G_t \cdot G_r \cdot \lambda^2}{(4\pi R)^2 \cdot L}, \quad (1.16)$$

де G_t , G_r – коефіцієнти підсилення антен передавача й приймача, λ – довжина хвилі сигналу, [м], $\lambda = c/f$, де c – швидкість світла, R – відстань між передавачем і приймачем, [м], L – коефіцієнт загальних втрат у системі (для спрощення розрахунків приймемо $L = 1$), P_t – потужність передавача (Вт), P_r – прийнята енергія сигналу у Ват-секундах (Вт·с).

Враховуючи час T_d , протягом якого приймається сигнал його визначимо енергію:

$$E_r = \left(\frac{P_t \cdot G_t \cdot G_r \cdot \lambda^2}{(4\pi R)^2 \cdot L} \right) \cdot T_d. \quad (1.17)$$

На рис. 1.5 представлено графіки, які демонструє лінії рівня прийнятої енергії сигналу (в дБ) залежно від R та T_d . З графіків бачимо, що зі збільшенням відстані прийнята енергія падає квадратично, що відображає класичну залежність згасання сигналу:

$$P_r \propto \frac{1}{R^2}. \quad (1.18)$$

Залежність (1.18) означає, що навіть незначне збільшення відстані значно знижує ймовірність виявлення сигналу приймачем розвідки.

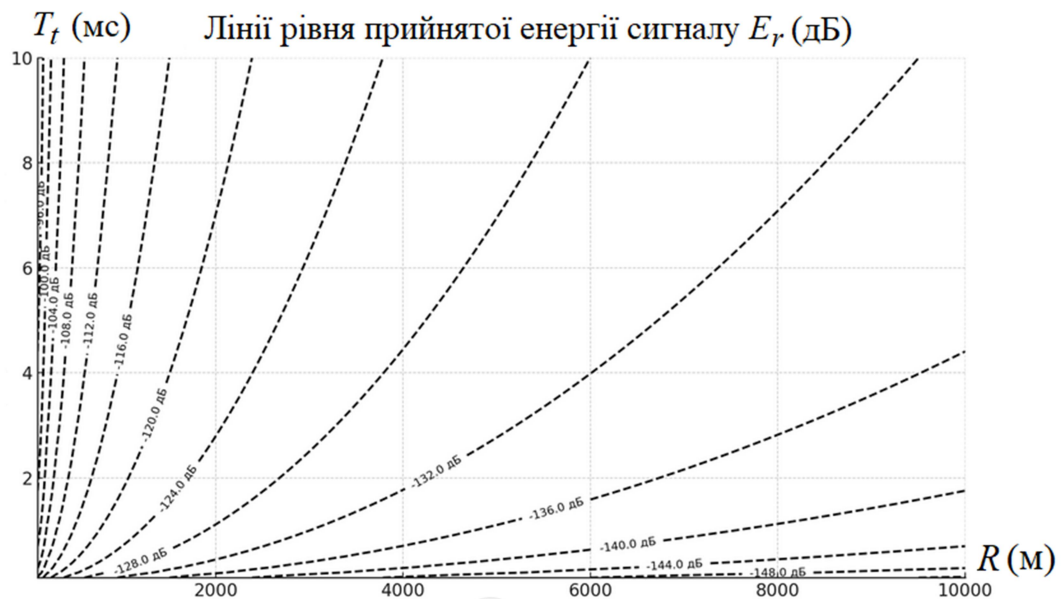


Рисунок 1.5 – Залежності лінії рівня прийнятої енергії сигналу E_r від R та T_d

Зі збільшенням часу перебування T_d прийнята енергія зростає лінійно, тобто:

$$P_r \propto T_d. \quad (1.19)$$

Отже, довший інтервал часу дозволяє накопичити більше енергії та спрощує виявлення сигналу станції з ППРЧ. Вочевидь, щоб компенсувати втрату енергії через збільшення відстані, потрібно збільшувати T_d . Це суперечить вимогам забезпечення енергетичної прихованості. Для наочності визначення оптимальної області параметрів для забезпечення енергетичної прихованості системи зв'язку з ППРЧ на рис. 1.6 представлено залежності отриманої енергії E_r в логарифмічній шкалі від R та T_d . Можна відзначити, що при зменшенні часу перебування на одній частоті сигнал стає менш енергетично «помітним» [32], однак і енергія сигналу на приймальній стороні зменшується. Збільшення відстані призводить до значного зниження рівня сигналу через квадратичну залежність. Оптимальна область прихованого, але надійного зв'язку – це баланс між малим часом перебування для забезпечення достатнього рівня енергетичної прихованості і достатнім рівнем енергії для прийому сигналу.

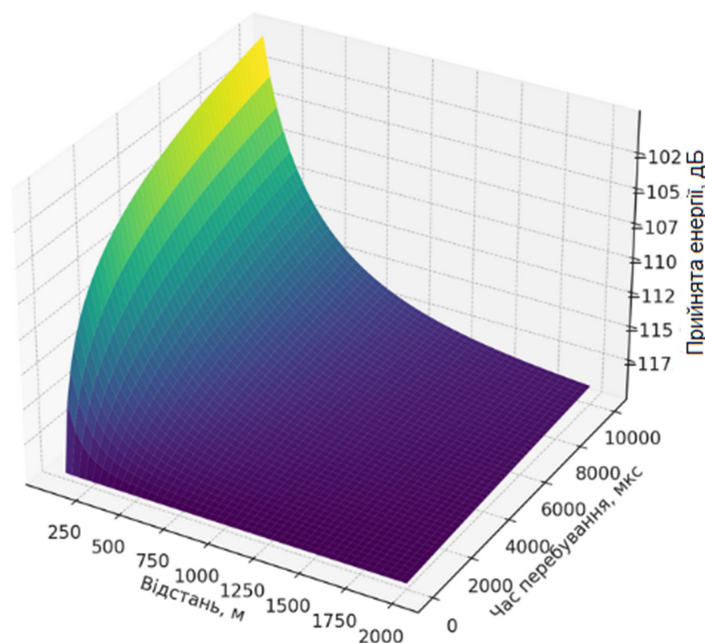


Рисунок 1.6 – Залежності отриманої енергії E_r для приймача з ППРЧ в логарифмічній шкалі від R та T_d

Таким чином, традиційна перевага ППРЧ у вигляді прихованості сигналу суттєво зменшується, що потребує удосконалення методів маскування,

адаптації частотних перестановок і застосування комбінованих методів спектрального розширення. Результати дослідження показали, що енергетична прихованість реалізується переважно через оптимізацію спектральної форми сигналу, зниження його потужності та використання складних методів модуляції, що ускладнюють виявлення передачі навіть за умови контролю радіочастотного середовища. У системах військового зв'язку та спецзв'язку ці методи дозволяють забезпечити стійкість до радіоелектронної розвідки та спостереження. Прикладами таких систем зв'язку можуть бути радіостанції P-002, P-005, P-030, P-030. Також можна відзначити, що технологія FHSS використовується у технології Bluetooth (IEEE 802.15.1), а також у військових радіостанціях сімейства корпорації Harris Corporation. Крім того, цей метод також знайшов своє використання у перших версіях протоколів Fi-Wi (IEEE 802.11). В ІКС з кодовим розділенням каналів була використана технологія DSSS, що спричинило появу систем cdmaOne, cdma2000, WCDMA та WiFi 802.11 b, g, ZigBee 802.15.4 [1, 2].

1.2.3. Метод розширення спектра на основі лінійної частотної модуляції

Метод формування широкосмугового сигналу на основі ЛЧМ використовує частоту [31], яка змінюється лінійно з часом у межах заданої смуги. Такі сигнали широко застосовуються в радіолокації, зв'язку, а також у системах із широким спектром. Математична модель ЛЧМ-сигналу визначається як:

$$s_{\text{ЛЧМ}} = A \cdot \cos(2\pi f_0 t + \pi \mu t^2), \quad 0 \leq t \ll T \quad (1.20)$$

де A – амплітуда сигналу, f_0 – початкова частота, $\mu = \frac{\Delta f}{T}$ – швидкість зміни частоти, Δf – смуга частот, T – тривалість імпульсу. Базою ЛЧМ-сигналу називається добуток смуги частот на тривалість сигналу:

$$B_{\text{ЛЧМ}} = \Delta f \times T. \quad (1.21)$$

Параметр $B_{\text{ЛЧМ}}$ визначає роздільну здатність сигналу та ступінь розширення спектра. Також по значенню $B_{\text{ЛЧМ}}$ можна оцінювати структурну прихованість, тобто чим вища база – тим складніше розпізнати структуру сигналу. Важливим показником ЛЧМ-сигналу є його спектральна щільність потужності. Енергетичне розширення ЛЧМ-сигналу розподіляє потужність P на широку смугу частот:

$$S(f) \approx \frac{P}{\Delta f}, \quad f_0 - \frac{\Delta f}{2} \leq f \leq f_0 + \frac{\Delta f}{2}. \quad (1.22)$$

Отже, можна зробити висновок, що чим нижче значення спектральної щільності потужності $S(f)$, тим важче виявити сигнал, який має більшу енергетичну прихованість.

Розглянемо енергетичну прихованість ЛЧМ сигналу. Вочевидь, що сигнал із великою базою $B_{\text{ЛЧМ}}$ має розосереджену потужність у спектрі, отже його складніше відрізнити від шуму. При цьому вся енергія сигналу все одно зосереджена в широкій смузі частот. Розглянемо оцінку ймовірності виявлення сигналу ЛЧМ. Вважаємо, що потужність сигналу розподілена по спектру, тоді сигнал важче відрізнити від шуму, якщо:

$$\frac{P}{\Delta f} \ll N_0, \quad (1.23)$$

де: N_0 – спектральна щільність шуму. Прийнята енергетична модель сигналу на приймальній стороні аналогічна виразу (1.17). На рис. 1.7 для визначення оптимальної області параметрів забезпечення енергетичної прихованості системи зв'язку з ЛЧМ представлено залежності отриманої енергії E_r в від смуги частот Δf , тривалістю сигналу T_d та бази сигналу $B_{\text{ЛЧМ}}$. Аналіз рис. 1.7 дозволяє зробити наступні висновки. Метод передавання на основі ЛЧМ

забезпечує енергетичну прихованість за рахунок зниження спектральної щільності.

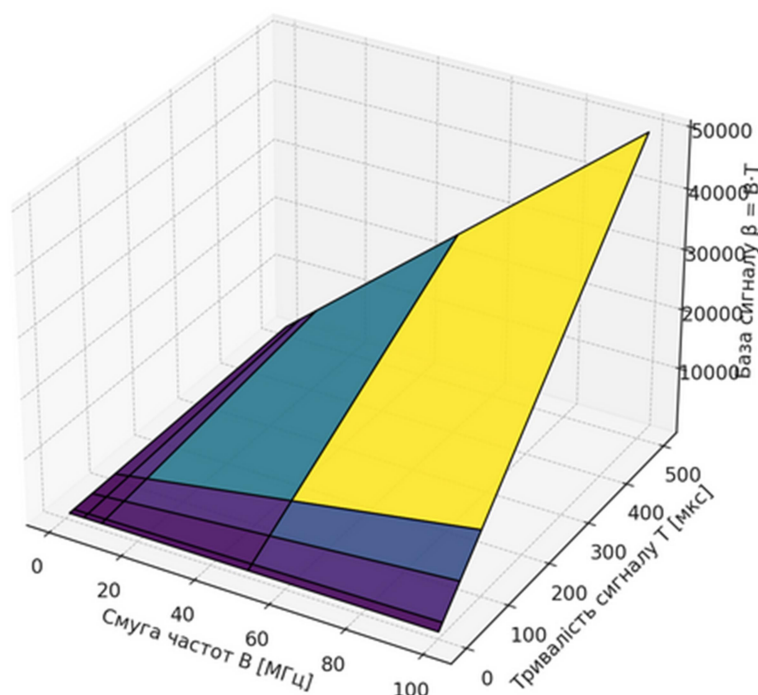


Рисунок 1.7 – з ЛЧМ від Δf , T_d та $B_{\text{лчм}}$

Велика значення бази сигналу підвищує структурну складність сигнальної конструкції, а отже – збільшується структурна прихованість. При цьому зберігається здатність прийому ЛЧМ-сигналу приймачем за умови вибору оптимальних параметрів передачі. Проте за надто великого розширення спектра можуть виникати апаратні обмеження, пов'язані з шириною смуги фільтрів, обробкою сигналу, тощо.

1.2.4. Забезпечення структурної прихованості сигнальних конструкцій

Структурна прихованість реалізується за рахунок ускладнення або повного унеможливлення визначення структури сигналу [4, 18], його параметрів і віднесення до певного класу або формату зразків, відомих противнику. Це особливо важливо у випадках, коли сигнал уже було виявлено,

тобто противником вирішена проблема енергетичної прихованості, але ще є можливість не допустити розпізнавання його типу або призначення. Для кількісного опису структурної прихованості можна використовувати ентропію сигналу:

$$H_s = - \sum_{i=1}^L p_i \cdot \log_2 p_i, \quad (1.24)$$

де p_i – ймовірність появи певного структурного стану або параметра (наприклад, фази, частоти, тощо), L – кількість станів або параметрів сигнальної конструкції. Отже ентропія сигналу H_s визначає міру невизначеності або складності сигнальної конструкції, що відображає кількість інформації, яку містить сигнал, та ступінь його випадковості. Високе значення ентропії сигналу свідчить про його високу структурну різноманітність, що ускладнює аналіз, класифікацію та виявлення закономірностей. У огляду структурної прихованості це означає, що чим вищою є ентропія, тим менше сигнал схожий на стандартні або відомі зразки, а отже, він є більш захищеним від розпізнавання та дешифрування сторонніми спостерігачами. Для оцінки складності сигналу, тобто низької подібності до відомих шаблонів сигнально-кодових конструкцій, доцільним є аналіз автокореляційної функції:

$$R_s = \mathbb{E}[s(t) \cdot s(t + \tau)]. \quad (1.25)$$

Для структурно прихованого сигналу характерна мале значення кореляції при $\tau \neq 0$, що вказує на відсутність періодичності або предикативності. Структурну прихованість можна оцінити через кількість можливих СКК, які здатна генерувати система, що ускладнює класифікацію сигналу. Для цього використовується бінарний логарифм, що дозволяє визначити кількість можливих двійкових комбінацій або структур сигналу:

$$H_{\text{стр}} = \log_2 N_{\text{ск}}, \quad (1.26)$$

де $H_{\text{стр}}$ – структурна ентропія, що характеризує рівень структурної прихованості сигналу, $N_{\text{ск}}$ – кількість можливих структур сигнально-кодкових комбінацій, які система може використовувати, наприклад, різні комбінації частот, фаз, амплітуд, тривалостей або форм модуляції.

Якщо L велике, тобто сигнал може набувати великої кількості різних форм, то логарифм $\log_2 N_{\text{ск}}$ також буде великим, що свідчить про високий рівень структурної прихованості. Така метрика відображає невизначеність для стороннього спостерігача – чим більша кількість варіантів, тим складніше ідентифікувати або класифікувати сигнал. Припустимо, система може формувати 1024 різні структури сигналу: $H_{\text{стр}} = \log_2 1024 = 10$ (дв. вим.). Це означає, що противнику потрібно проаналізувати $2^{10} = 1024$ варіанти для аналізу структури сигналу, що значно ускладнює розпізнавання.

Розглянемо загальну структурну прихованість з урахуванням дискретної послідовності та системи модуляції. При цьому потрібно враховувати кількість реалізацій сигнально-кодкових комбінацій та позиційність модуляції, тобто можливість передавати інформацію не тільки значенням символу, а й його позицією в часі, частоті або іншому параметричному просторі:

$$H_{\text{стр}} = \log_2 N_{\text{ск}} + \log_2 N_{\text{поз}}, \quad (1.27)$$

де $H_{\text{стр}}$ – оцінка структурної прихованості сигналу (дв. вим.), $N_{\text{ск}}$ – кількість можливих сигнально-кодкових комбінацій, тобто різновидів форми/структури сигналу, які може приймати система, $N_{\text{поз}}$ – кількість позиційних варіантів розміщення сигналів у просторі модуляції, наприклад, кількість можливих позицій імпульсів у часі, частоті, фазі тощо.

Розглянемо систему, яка здатна формувати 1024 різні структури сигналу та використовує модуляцію КАМ-8, тоді: $H_{\text{стр}} = \log_2 1024 + \log_2 8 = 10 + 3 = 13$ (дв. вим.), тобто, противнику потрібно проаналізувати $2^{13} = 8192$ варіанти для аналізу структури сигналу, що значно ускладнює розпізнавання.

Бачимо, що зростання кількості позицій L та/або параметричних станів сигнальних конструкцій приводить до збільшення структурної ентропії $H_{\text{стр}}$, що ускладнює задачу перехоплення та аналізу структури сигналу стороннім спостерігачем і підвищує рівень структурної прихованості.

Розглянемо узагальнену структурну прихованість з використанням при використанні технології прямого розширення спектра псевдовипадковими послідовностями (ПВП). В цьому випадку:

$$H_{\text{стр}} = \log_2 N_{\text{ск}} + \log_2 N_{\text{поз}} + \log_2 N_{\text{пвп}}, \quad (1.28)$$

де: $N_{\text{пвп}}$ – кількість можливих послідовностей розширення спектра, наприклад, кількість унікальних ПВП або частотних перестановок.

Отже, прихованість базується не лише на спектральному або енергетичному маскуванні, а й на ускладненні аналізу внутрішньої структури сигналу шляхом використання складних, змінних або випадкових закономірностей. Подальше підвищення структурної прихованості можливо за рахунок використання таймерних сигналів, квазівипадкових послідовностей або хаотичних коливань.

1.2.5. Забезпечення інформаційної прихованості даних

Інформаційна прихованість передбачає унеможливлення або істотне ускладнення розкриття семантичного змісту переданої інформації, навіть у випадку її повного або часткового виявлення, перехоплення та успішної демодуляції сигналу противником [33-35]. Тобто, навіть якщо злоумисник зможе ідентифікувати наявність передачі, локалізувати її джерело та отримати доступ до несучої частоти, формат кадру або протоколу, він не повинен мати змоги витягнути з переданих даних змістовну (семантичну) інформацію без знання секретного ключа або параметрів кодування.

Основною метою інформаційної прихованості є захист змісту інформаційного повідомлення M від несанкціонованого доступу навіть після дешифрування або відновлення сигналу $s(t)$, тобто забезпечення:

$$P(\hat{M} = M | s(t), A_{\text{ан}}) \approx 0, \quad (1.29)$$

де M – оцінка повідомлення, яку намагається отримати зловмисник, $s(t)$ – сигнал, що передається в каналі, $A_{\text{ан}}$ – позначає можливість наявності у зловмисника засобів аналізу сигналу та алгоритмів обробки.

Загальний рівень інформаційної прихованості можна оцінити через ентропійні міри – зокрема, залишкову ентропію повідомлення при умовному знанні сигналу:

$$H(M | s(t)) \approx H(M) \quad (1.30)$$

Це означає, що навіть після перехоплення сигналу $s(t)$ рівень невизначеності щодо змісту повідомлення M не зменшується – тобто перехоплення сигналу не дає зловмиснику корисної інформації.

Для підвищення інформаційної прихованості застосовуються такі методи:

1) криптографічне перетворення повідомлень:

$$S_{\text{інф}} = E_K(M), \quad (1.31)$$

де E_K – алгоритм шифрування з ключем K , $S_{\text{інф}}$ – зашифроване повідомлення;

2) модуляція інформації на основі хаотичних коливань:

$$s(t) = f(C, \phi(t)), \quad (1.32)$$

де $\phi(t)$ – хаотична несуча складова;

3) спектральне розширення: застосовується для перетворення вузькосмугового сигналу в широкосмуговий, знижуючи його спектральну щільність потужності.

При великому значенні часово-частотної бази $B_{\text{ПВП}}$, переданий сигнал набуває шумоподібного вигляду, тобто має розсіяну спектральну потужність та низьку корельованість з будь-якими відомими тестовими сигналами. Це значно ускладнює процедури виявлення, демодуляції, ідентифікації та подальшого аналізу сигналу з боку злоумисника, навіть при використанні сучасних засобів радіоелектронної розвідки. Застосування ПВП [35, 36] невідомої або змінної структури як основи для модуляції або формування сигнально-кодових конструкцій дозволяє забезпечити криптографічну стійкість сигналу вже на першому та другому рівнях моделі OSI (фізичному та каналному). Зокрема, реалізуються наступні властивості:

- 1) нестабільність і непередбачуваність сигналу в часі та частоті;
- 2) інформаційна невизначеність структури кадру, формату пакету або послідовності;
- 3) інерційність до атак типу «спостереження», коли злоумисник намагається відновити структуру ПВП або її період;
- 4) високий рівень ентропії сигналу, наближений до ентропії білого шуму:

$$H(s(t)) \approx H_{\text{шум}}. \quad (1.33)$$

Це забезпечує багаторівневу прихованість: від складності виявлення сигналу в радіоефірі до неможливості семантичної інтерпретації змісту повідомлення без знання параметрів формування ПВП, ключів шифрування або алгоритмів перетворення. Крім того, завдяки відсутності у сигналі стандартних структурних елементів (преамбули, заголовків тощо), ускладнюється його прийом навіть у разі повної синхронізації за частотою та часовими характеристиками передачі. Отже, у системах зв'язку з адаптивною побудовою сигнально-кодових конструкцій на основі ПВП невідомої структури

відбувається: інтеграція криптографічного захисту на фізичному рівні; зменшення потреби в традиційних методах шифрування на вищих рівнях моделі OSI; підвищення завадостійкості та інформаційної стійкості системи до атак перехоплення, аналізу та моделювання сигналу. Такі підходи є надзвичайно актуальними для систем зв'язку, що працюють в умовах РЕБ [37, 38], де критично важливим є не лише захист змісту повідомлення, а й сам факт ведення передачі, який повинен залишатись максимально непомітним або складним для виявлення злоумисником. Таким чином, інформаційна прихованість реалізується як на інформаційному рівні за допомогою шифрування, так і на сигнальному рівні з використанням модуляції та спектрального розширення, створюючи багаторівневий захист семантичного змісту повідомлення в умовах загроз перехоплення.

1.3. Вплив параметричного перетворення сигнально-кодових конструкцій на захист інформації

Параметричне перетворення сигнально-кодових конструкцій (СКК) є ефективним засобом для забезпечення адаптивності, завадостійкості та конфіденційності передачі інформації в ІКС. Основною ідеєю такого підходу є модифікація одного або декількох параметрів сигналу, що передається, відповідно до заданих алгоритмів або функцій перетворення [39-41]. До основних параметрів, що піддаються перетворенню, відносяться: амплітуда A , частота f , фаза ϕ , тривалість імпульсу τ , положення імпульсу в часі t_0 , спектральна ширина сигналу Δf , порядок або позиція слів у кодовій комбінації, відношення сигнал/шум (SNR) на приймальній стороні. Прикладом такого перетворення є пряме розширення спектра, яке здійснюється шляхом модуляції інформаційних біт за допомогою ПВП [36]. Це призводить до значного збільшення спектральної ширини сигналу:

$$\Delta f_{\text{розш}} \approx \frac{1}{\tau_{\text{чип}}}, \quad (1.34)$$

де: $\tau_{\text{чип}}$ – тривалість чіпу ПВП, яка значно менша за тривалість символу інформаційної послідовності.

Сигнал після ПРС матиме наступний вигляд:

$$s(t) = \sum_N b_N c_N p(t - N\tau_{\text{чип}}), \quad (1.35)$$

де $b_N \in \{-1, +1\}$ – інформаційні символи, $c_N \in \{-1, +1\}$ – елементи ПВП, $p(t)$ – еталонний імпульс.

Однією з переваг такого перетворення є зменшення ймовірності виявлення сигналу, оскільки його спектральна щільність потужності розподіляється на ширшу смугу частот. Це ускладнює виділення сигналу на фоні шуму або завад [32-35]. Крім того, можуть застосовуватись такі методи параметричного перетворення:

1) ППРЧ, коли передача інформації здійснюється на різних частотах згідно з визначеною або псевдовипадковою схемою:

$$f_i(t) = f_0 + i \cdot \Delta f, \quad i \in \{0, 1, \dots, N - 1\}; \quad (1.36)$$

2) фазові перестановки в рамках кодування, наприклад, фазова маніпуляція, що забезпечує більш ефективне використання каналу:

$$s(t) = A \cdot \cos(2\pi f_0 t + \phi_n), \quad (1.37)$$

де ϕ_n – фазовий зсув, що відповідає передаваному біту або символному поєднанню.

У випадку застосування таймерного кодування [25, 26], зміна параметрів ТСК може відбуватись за рахунок варіацій у часових інтервалах між

імпульсами. Нехай основою сигнальної конструкції є послідовність імпульсів із часовими інтервалами $\{T_i\}$, які несуть інформаційне навантаження. У загальному випадку, параметричне перетворення може бути представлене як функція:

$$T'_i = f_p(T_i, \theta), \quad (1.38)$$

де T_i – перетворений часовий інтервал, f_p – функція параметричного перетворення, θ – вектор параметрів перетворення, наприклад, коефіцієнт масштабування, зміщення, стохастична компонента тощо.

Параметричне перетворення [40, 41] дозволяє модулювати часову структуру сигналу з урахуванням: адаптації до потокового стану каналу зв'язку; забезпечення певних показників прихованості для ускладнення виявлення сеансу передавання інформації засобами РЕР; можливості підвищення ентропії сигналу; реалізації хаотичних або квазіхаотичних структур для маскування повідомлень тощо. Розглянемо приклад застосування стохастичного параметричного перетворення [44-46]:

$$T'_i = T_i \cdot (1 + \delta_i), \quad (1.39)$$

де δ_i – випадкова величина з нормальним або рівномірним законом розподілу, яка вводить елемент псевдовипадковості у часову структуру сигналу. Це дозволяє знизити кореляцію між елементами конструкції та підвищити її криптостійкість. Важливо зазначити, що при правильному узгодженні параметрів перетворення між передавачем і приймачем забезпечується правильне детектування сигналу навіть при великих рівнях завад в каналі, що підтверджується розрахунками середньої ймовірності правильного приймання:

$$P_d = \int_0^\infty p_T(t) \cdot \Lambda(t) dt, \quad (1.40)$$

де $p_T(t)$ – щільність розподілу тривалостей після перетворення, $\Lambda(t)$ – функція виявлення, яка визначається характеристиками фільтрації на приймальній стороні.

У випадку застосування позиційного кодування, перетворенням може бути динамічне перенумерування позицій активних елементів у кодовій комбінації, що описується перестановкою:

$$X' = \Pi(X), \quad (1.41)$$

де X – вхідна бітова послідовність, Π – оператор перестановки, реалізований на основі ПВП або параметричного закону.

Завдяки параметричному перетворенню досягається зменшення ймовірності перехоплення сигналу та впливу вузькосмугових завад, тобто підвищується енергетична прихованість передаваних сигнальних конструкцій. Високоєфективна реалізація параметричних перетворень можлива при використанні цифрової обробки сигналів (ЦОС), що дозволяє динамічно змінювати параметри СКК на рівні програмного забезпечення. Отже, параметричні перетворення СКК виступають важливим інструментом для реалізації захищених та адаптивних систем зв'язку, особливо в умовах дії навмисних радіоелектронних перешкод або при потребі забезпечення секретності передачі інформації.

1.4. Модель оцінювання захищеності передачі інформації на основі обсягу сигналу

У процесі функціонування інформаційного каналу використовуються такі ключові характеристики, як швидкість введення інформації, швидкість передавання інформації та пропускна здатність каналу [47-49]. Швидкість введення інформації – це середня кількість інформації, що надходить від джерела повідомлень до інформаційного каналу за одиницю часу [50]:

$$R_{\text{вв}} = \lim_{t \rightarrow \infty} \frac{H(X_1, X_2, \dots, X_t)}{t} \quad (1.42)$$

де $H(X_1, X_2, \dots, X_t)$ – ентропія послідовності повідомлень джерела за час t . Це характеристика джерела повідомлень і залежить виключно від статистичних властивостей сформованих повідомлень. Швидкість передавання інформації через канал визначається як середня кількість інформації, яка дійсно передається через канал за одиницю часу [50]:

$$R_{\text{пер}} = \lim_{t \rightarrow \infty} \frac{I(X; Y)}{t}, \quad (1.43)$$

де $I(X; Y)$ – взаємна інформація між переданим сигналом X і прийнятим сигналом Y , що відображає кількість корисної (не спотвореної) інформації, переданої через канал.

Пропускна здатність каналу – це максимальна теоретично досяжна швидкість передавання інформації через канал зв'язку при оптимальному кодуванні [50]:

$$C = \max_{P(X)} I(X; Y), \quad (1.44)$$

де максимум береться за всіма можливими розподілами вхідного алфавіту $P(X)$. Це характеристика самого каналу і не залежить від статистики повідомлень. Розглянемо умови ефективної передачі, що передбачає досягнення максимально ефективного використання каналу. Для цього необхідно виконати дві умови:

1) швидкість передавання інформації повинна бути максимально наближеною до пропускної здатності [50]:

$$R_{\text{пер}} \leq C; \quad (1.45)$$

2) швидкість введення інформації не повинна перевищувати пропускну здатність каналу:

$$R_{\text{вв}} \leq C. \quad (1.46)$$

У протилежному разі відбуватиметься втрата інформації, тобто не вся інформація буде успішно передана або доставлена. Ці вимоги визначають динамічну узгодженість джерела повідомлень і інформаційного каналу. Сучасні інформаційні системи у військовій та критичній інфраструктурі мають забезпечувати не лише ефективну, але й захищену передачу інформації [19, 33]. Одним із перспективних підходів до оцінювання захищеності передачі інформації є використання інтегрального параметра сигналу, що поєднує його часові, частотні та енергетичні характеристики. Таким параметром є обсяг сигналу, який дозволяє встановити умови надійної та прихованої передачі даних через канал зв'язку. Узагальнені характеристики сигналу [50, 51] можуть бути представлені параметрами, які характеризують інформаційний сигнал у процесі передачі, є: тривалість сигналу T_c , що визначає час зайнятості каналу; ширина спектру F_c , що визначає частотний діапазон сигналу; динамічний діапазон сигналу D_c , що відображає співвідношення потужності сигналу до потужності завади, зазвичай виражене в логарифмічній формі:

$$D_c = \log_2 \left(\frac{P_c}{P_\xi} \right) \quad (1.47)$$

де P_c – середня потужність сигналу, P_ξ – середня потужність завад.

На основі цих трьох параметрів визначається обсяг сигналу:

$$V_c = T_c \times F_c \times D_c. \quad (1.48)$$

У просторовій інтерпретації обсяг сигналу можна подати у вигляді паралелепіпеда (рис. 1.8), кожне ребро якого відповідає одному з параметрів сигналу. Ємність інформаційного каналу також характеризується аналогічними параметрами: 1) допустимий час передачі через канал T_c ; пропускна смуга каналу F_c ; динамічний діапазон каналу D_c . На їх основі визначається ємність каналу:

$$V_k = T_k \times F_k \times D_k. \quad (1.49)$$

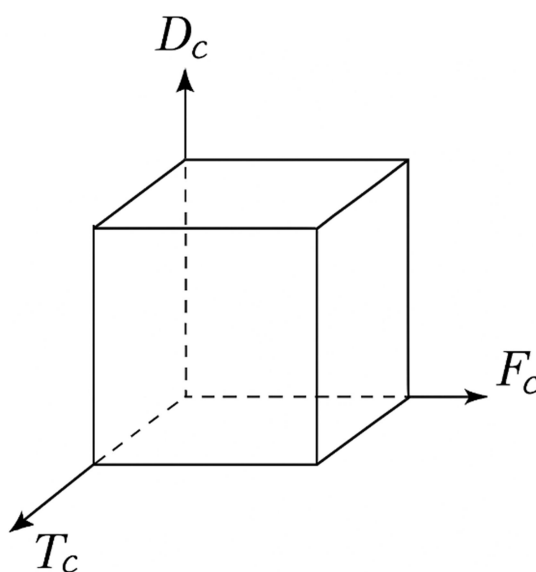


Рисунок 1.8 – Геометрична модель обсягу сигналу
з параметрами T_c , F_c та D_c

Розглянемо умову забезпечення безпечної передачі. Передача сигналу без втрати даних та із збереженням конфіденційності можлива за умови, що обсяг сигналу не перевищує ємність каналу:

$$V_c \leq V_k. \quad (1.50)$$

На рис. 1.9. зображено просторову інтерпретацію обсягу сигналу як паралелепіпеда з ребрами T_c , F_c , D_c , які відповідають тривалості сигналу,

ширині спектра та динамічному діапазону відповідно. Усередині зображено менший паралелепіпед, що відображає ємність каналу з параметрами T_K , F_K , D_K . Для забезпечення надійної передачі інформації без спотворень обсяг сигналу повинен повністю вміщуватися в ємність каналу, тобто виконуватись умова:

$$T_c \leq T_K, \quad F_c \leq F_K, \quad D_c \leq D_K \quad (1.51)$$

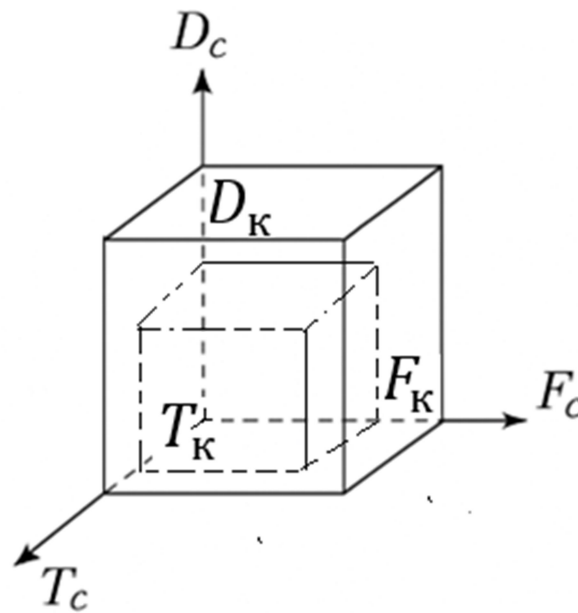


Рисунок 1.9 – Геометрична модель узгодження обсягу сигналу з ємністю каналу

Ця модель дозволяє наочно оцінювати відповідність характеристик сигналу можливостям каналу та приймати рішення щодо методів узгодження або параметричного перетворення сигналу. Однак у контексті інформаційної безпеки ця умова також може трактуватись як умова допустимого рівня енергетичної та структурної прихованості сигналу у каналі. Наддамо оцінку захищеності з урахуванням умови (1.50). В рамках запропонованої аналітичної моделі, чим менше значення обсягу сигналу V_c – тим нижча ймовірність його виявлення стороннім спостерігачем або перехоплення. Таким чином, обсяг сигналу використовується як показник фізичного рівня захисту.

Розглянемо критерії підвищеної захищеності передачі сигналу:

- 1) зменшення тривалості передачі сигналу:

$$T_c \rightarrow \min ; \quad (1.51)$$

2) розширення спектру за допомогою різних методів ПРС, ППРЧ та ЛЧМ:

$$F_c \rightarrow \min ; \quad (1.52)$$

3) маскування енергетики сигналу завдяки низької потужності передавача:

$$D_c \rightarrow \min . \quad (1.53)$$

Зменшення обсягу сигналу, наприклад, шляхом прямого розширення спектра T_c зменшується, а F_c збільшується, при цьому V_c може не змінитися або навіть зменшитися, що ускладнює перехоплення та аналіз сигналу. Збільшення ширини спектра F_c або зменшення тривалості імпульсу T_c знижує щільність енергії сигналу, що зменшує ймовірність його виявлення на тлі завад – тобто покращує енергетична прихованість передачі. Високий динамічний діапазон D_c може сприяти кращій стійкості до завад, але також є параметром, який можна регулювати з метою зниження ймовірності успішного перехоплення. Отже, аналіз обсягу сигналу як тривимірної метрики дозволяє не лише оцінити ефективність передачі, а й надати кількісну оцінку рівню захищеності інформації в каналі. Аналітична модель оцінювання захищеності передачі інформації на основі обсягу сигналу дозволяє:

- 1) інтегрувати фізичні параметри сигналу в єдиний показник захищеності;
- 2) здійснювати порівняння сигнальних конструкцій з позиції їх вразливості до виявлення;
- 3) обґрунтовано вибирати параметри модулювання, кодування та спектральної обробки сигналів для забезпечення високого рівня інформаційного захисту.

1.5. Ресурси каналу зв'язку та умови забезпечення захищеності інформаційно-комунікаційних систем

1.5.1. Вплив засобів РЕБ на ресурсні вимоги і захищеність каналів зв'язку

В умовах радіоелектронного протистояння [52, 53] особливої актуальності набуває розробка та впровадження інформаційно-комунікаційних систем, здатних забезпечувати високий рівень захищеності каналу зв'язку від засобів радіотехнічної розвідки, навмисних перешкод і несанкціонованого доступу з боку противника. Одним із ключових напрямів підвищення захищеності таких систем є реалізація багаторівневого захисту переданої інформації, що передбачає використання різноманітних методів та засобів сигнально-кодових перетворень і криптографічних рішень. Кожен рівень захисту базується на певному наборі технічних і алгоритмічних засобів, що впливають на характеристики сигналу та даних у каналі зв'язку. З метою об'єктивної оцінки ефективності реалізованих заходів доцільно впроваджувати систему кількісних та якісних критеріїв. Основними критеріями ефективності обрано показники завадозахищеності, серед яких: завадостійкість; енергетична прихованість; структурна прихованість. У дослідженні проведено аналіз впливу різних методів підвищення енергетичної та структурної прихованості на загальну завадостійкість системи зв'язку. Особливу увагу приділено оцінці змін у частотній та енергетичній ефективності каналу в умовах застосування захисних перетворень. Запропонована система критеріїв дозволяє здійснювати порівняльний аналіз альтернативних методів захисту інформації з урахуванням вимог замовника до рівнів завадостійкості, прихованості передачі та ефективного використання ресурсів каналу зв'язку.

Розглянемо ІКС, які забезпечують взаємодію між військовими підрозділами в умовах РЕБ [9, 54] та повинні гарантувати високий рівень захищеності каналів зв'язку від засобів РЕР і НСД. Як було зазначено раніше,

більшість існуючих методів захисту інформації від НСД реалізуються переважно на вищих рівнях еталонної моделі OSI – зокрема, на рівнях представлення та прикладному, за рахунок використання криптографічних засобів (таких як ГОСТ 28147-89, AES, DES тощо) [34, 35]. Водночас процес передавання сигналу відбувається через фізичне середовище, і саме на нижніх рівнях – фізичному та каналному – існує ризик виявлення, перехоплення та подальшого аналізу переданої інформації. У зв'язку з цим останнім часом активно розвиваються підходи до захисту, орієнтовані на нижні рівні моделі OSI [34]. Це, зокрема, методи формування сигналів зі структурною або енергетичною прихованістю, використання шумоподібних або хаотичних сигналів [36, 37], методи маскування та спектрального розширення.

Вочевидь, що впровадження багаторівневої моделі захисту, яка охоплює як фізичний, так і логічні рівні, дозволяє комплексно підвищити стійкість ІКС до розвідки та атак. В умовах радіоелектронного протистояння це стає критично важливим. З метою мінімізації ризиків компрометації переданої інформації кожен рівень має бути забезпечений власним арсеналом засобів сигнально-кодових перетворень та захисних механізмів, адаптованих до характеру можливих загроз.

Відомо [1-3], що ефективність методів захисту інформації, реалізованих на каналному та фізичному рівнях, доцільно оцінювати за допомогою показників завадозахищеності, зокрема – прихованості та завадостійкості. При цьому вибір конкретних методів повинен здійснюватися з урахуванням взаємного впливу між цими показниками. Зокрема, реалізація високого рівня завадостійкості може впливати на зниження прихованості (наприклад, шляхом збільшення енергетичного спектра сигналу), і навпаки. До основних складових прихованості слід віднести: енергетичну, структурну та інформаційну. Крім того, слід враховувати характер і інтенсивність РЕБ, а також передбачувані дії противника, які можуть включати виявлення, аналіз, перехоплення, дешифрування або активне придушення радіоканалу [2]. У зв'язку з цим актуальною науково-прикладною задачею є розробка інтегрованої системи

оцінювання ефективності методів захисту інформації, яка враховує показники як прихованості, так і стійкості до засобів РЕБ. Метою дослідження є розробка формалізованої системи оцінок рівня захищеності методів передавання інформації на фізичному і каналному рівнях, яка базується на показниках прихованості та завадостійкості, і дозволяє адекватно оцінювати ефективність захисту в умовах різних сценаріїв РЕБ.

Система оцінювання повинна ґрунтуватися на чітко визначених критеріях ефективності, що відображають: рівень протидії засобам РЕБ; здатність протистояти НСД; збереження працездатності системи зв'язку у присутності навмисних або фонових завад. У типовому сценарії протидії, противник здійснює виявлення радіосигналу за допомогою засобів РЕБ, а потім застосовує активне придушення шляхом генерації цілеспрямованої завади. Такий сценарій є відносно простим і передбачає мінімальний обсяг аналітичних або технічних дій з боку противника. Проте навіть у такому випадку ефективність системи захисту повинна забезпечувати недопущення або ускладнення реалізації цього процесу. Отже, досягнення високої захищеності каналів зв'язку в системах СПУ вимагає багаторівневого підходу, заснованого на комплексному аналізі взаємозалежних показників прихованості та завадостійкості в умовах динамічно змінного середовища РЕБ [38, 39].

Більш складний сценарій протидії передбачає розкриття змісту конфіденційної інформації, що вимагає вирішення низки послідовних завдань: виявлення сигналу в радіоканалі та його перехоплення, тобто фіксація на носії інформації; аналіз і розпізнавання структури сигналу: формат кадру, тип модуляції, схема мультиплексування тощо; дешифрування переданої інформації з метою отримання її змісту. Такий сценарій протидії може мати різні варіанти розвитку, залежно від кінцевої мети противника: пасивне прослуховування, тобто отримання повідомлення без втручання у процес зв'язку; активне втручання з подальшою модифікацією повідомлення та імітацією роботи передавача, з метою дезінформації абонентів ІКС.

Залежно від обраної стратегії РЕБ противника, на етапі проектування ІКС доцільно реалізовувати різні типи прихованості, які підвищують стійкість системи до виявлення, перехоплення та дешифрування. Енергетична прихованість досягається шляхом застосування сигнальних конструкцій з маскувальними властивостями, які знижують ймовірність виявлення сигналу засобами радіотехнічної розвідки. Для цього використовуються методи розширення спектра вузькосмугових інформаційних сигналів, такі як: ППРЧ; ПРС за допомогою ПВП; ЛЧМ; комбіновані методи з одночасним застосуванням ППРЧ і ПВП; інші варіанти багатоканального або хаотичного спектрального розподілу. Структурна прихованість забезпечується модифікацією або маскуванням протокольної структури передавання, що ускладнює її розпізнавання при аналізі захопленого сигналу. Інформаційна прихованість реалізується шляхом криптографічного шифрування повідомлень та/або стеганографічного кодування, що унеможлиблює відновлення змісту навіть у разі успішного перехоплення сигналу.

Отже, ефективна система захисту інформації в умовах складного сценарію протидії повинна інтегрувати багаторівневі механізми прихованості з урахуванням прогнозованих можливостей противника та типового сценарію РЕБ.

1.5.2. Система оцінювання методів захисту інформації

Система оцінювання ефективності методів захисту інформації має ґрунтуватися на критеріях ефективності [1, 2], що відображають здатність протидіяти засобам РЕБ і НСД. У межах РЕБ [13] можуть реалізовуватися різні сценарії впливу на роботу ІКС. Найпростіший сценарій передбачає лише виявлення сигналу противником із подальшим його придушенням за допомогою спрямованої завади. Такий тип протидії має обмежену кількість завдань для зловмисника. Натомість більш складні сценарії орієнтовані на розкриття змісту переданої інформації та включають послідовність дій:

виявлення сигналу, його перехоплення [15], аналіз структури сигнально-кової конструкції, а також дешифрування. Подальший розвиток таких атак може передбачати прослуховування повідомлень або їхню модифікацію з метою імітації легітимного передавача в системі зв'язку. Залежно від складності сценарію дій противника на етапі проєктування ІКС доцільно впроваджувати різні види прихованості: енергетичну, структурну та інформаційну. Усі ці аспекти мають бути інтегровані в узагальнену модель захисту, що базується на параметричному перетворенні сигнально-кодових конструкцій.

Енергетична прихованість забезпечується завдяки використанню сигнально-кодових конструкцій, які мають властивості маскуванню, що ускладнює їх виявлення засобами РЕР у радіоканалі. Для цього застосовуються методи параметричного перетворення вузькосмугових сигналів, зокрема: ППРЧ, ПРС за допомогою ПВП, ЛЧМ, а також комбіновані методи розширення спектра. У результаті вузькосмуговий сигнал із базою $B_y \approx 1$ перетворюється на широкосмуговий з $B_{ш} \gg 1$. Маскувальний ефект досягається, коли амплітуда або спектральна щільність корисного сигналу знижується до рівня шуму в каналі, що робить його виявлення ускладненим.

Енергетична прихованість забезпечується завдяки використанню сигнально-кодових конструкцій, які мають властивості маскуванню, що ускладнює їх виявлення засобами РЕР у радіоканалі. Для цього застосовуються методи параметричного перетворення вузькосмугових сигналів, зокрема: псевдовипадковий перескок (ППРЧ), пряме розширення спектра (ПРС) псевдовипадковими послідовностями (ПВП), лінійна частотна модуляція (ЛЧМ), а також комбіновані методи розширення спектра. У результаті вузькосмуговий сигнал із базою $B_y \approx 1$ перетворюється на широкосмуговий з базою $B_{ш} \gg 1$. Маскувальний ефект досягається, коли амплітуда або спектральна щільність корисного сигналу знижується до рівня шуму в каналі, що робить його виявлення ускладненим.

Оцінимо взаємозв'язок між умовою забезпечення необхідної достовірності передачі і енергетичної прихованості сигнальних конструкцій для методу прямого розширення спектра ПВП. Розглянемо теорему Шеннона про пропускну спроможність каналу:

$$C = \Delta F \log_2 \left(1 + \frac{P_c}{P_{\text{ш}}} \right) \quad (1.54)$$

де ΔF – смуга частот, яка призначена для передавання даних, P_c – потужність сигналу на виході передавача, $P_{\text{ш}}$ – потужність завади в каналі.

З виразу (1.54) випливає, що теоретично передавання інформації в каналі зв'язку можливе з будь-якою швидкістю, що не перевищує пропускну здатність, і з будь-якою заданою достовірністю. Водночас забезпечення енергетичної прихованості можливе за таких умов:

$$\begin{cases} B_{\text{ш}} = T\Delta F \rightarrow \infty \\ P_c/P_{\text{ш}} \rightarrow 1 \end{cases} \quad (1.55)$$

та

$$P_c/P_{\text{ш}} \leq 1. \quad (1.56)$$

При виконанні (1.56) передавання здійснюється сигнальними конструкціями, рівень яких не перевищує потужність фону або змінюється за частотою настільки динамічно, що унеможлиблює їхнє надійне виявлення засобами РЕР. У такому випадку сигнал набуває властивостей малопомітності, що є ознакою реалізації максимальної енергетичної прихованості.

Водночас реалізація умов (1.55) та (1.56) має сенс лише за умови дотримання необхідної завадостійкості та мінімально допустимої швидкості передавання. Це вимагає побудови узагальненої моделі захисту інформації, яка дозволяє одночасно враховувати достовірність, енергетичну прихованість та ефективність використання каналу зв'язку.

Теорема. Існує взаємозв'язок між завадостійкістю передавання даних і умовами забезпечення енергетичної прихованості сигнальних конструкцій (1.55) і (1.56).

Доведення. Розглянемо другу частину теореми Шеннона, відповідно до якої для будь-якого рівня достовірності передавання існує код, що забезпечує завадостійку передачу даних із імовірністю помилки, близькою до нуля, за умови:

$$R < C = \Delta F \log_2 \left(1 + \frac{P_c}{P_{\text{ш}}} \right), \quad (1.57)$$

де R – швидкість передавання. Нехай для розширення спектра сигналу використовується псевдовипадкова послідовність, яка представлена у вигляді двійкового завадостійкого коду з параметрами:

$$n = k + r, \quad (1.58)$$

де k та r – кількість інформаційних і перевірочних елементів відповідно.

Відповідно до теореми Шеннона про кодування, якщо:

$$n \rightarrow \infty, \quad (1.59)$$

то й $k \rightarrow \infty$, але повільніше зростає лише r , що призводить до: зменшення частки контрольних елементів; зростання коригувальної здатності коду; збільшення достовірності передавання. Для наочності в табл. 1.1 наведені параметри циклічного коду.

Припустимо, що збільшення довжини кодового блоку n на інтервалі часу $T = nt_0$ здійснюється за рахунок зменшення тривалості одного елементу:

$$t_0 > t_0^*, \quad (1.60)$$

де t_0^* – тривалість елементу після кодування.

З урахуванням кодової швидкості $\gamma_k = k/n$, отримаємо:

$$t_0^* = \gamma_k t_0. \quad (1.61)$$

Таблиця 1.1 – Параметри циклічного коду

№	n	k	r	d_0	γ_k
1	7	4	3	3	0,571
2	15	11	4	3	0,733
3	31	21	10	5	0,733
4	63	45	18	7	0,714
5	127	99	28	9	0,779
6	255	215	40	11	0,843
7	511	430	261	19	0,841

Зменшення тривалості імпульсу призводить до зменшення енергії одного елемента сигналу, а отже – до зменшення помітності сигналу в радіоканалі (підвищення енергетичної прихованості). Разом із цим, швидкість передавання при розширенні спектра падає в n/k разів, що, однак, компенсується зростанням достовірності при необмеженій смузі частот $\Delta F \rightarrow \infty$. Зі збільшенням n кодова швидкість

$$\gamma_k \rightarrow 1, \quad (1.62)$$

і при цьому база широкосмутового сигналу збігається з довжиною послідовності, тобто:

$$B_{\text{ш}} = n \rightarrow \infty. \quad (1.63)$$

Таким чином, при збільшенні бази широкосмутового сигналу $B_{\text{ш}}$, що відповідає умові (1.63), забезпечується одночасне зростання достовірності передавання та енергетичної прихованості. Умова (1.60), тобто $P_c/P_{\text{ш}} \leq 1$, при

цьому виконується внаслідок зменшення енергії кожного імпульсу при збереженні або підвищенні рівня достовірності. Отже, виконання умов (1.55) та (1.56) вимагає застосування завадостійкого кодування великої довжини (із зростаючим n) та зменшення амплітуди елементів сигналу, що призводить до реалізації: високої енергетичної прихованості (сигнал зливається з фоновим шумом); високої достовірності (через підвищення завадостійкості). Це й треба було довести.

У реальних системах зв'язку з кодовим розділенням каналів в якості дозволених комбінацій для розширення спектра вузькосмугового сигналу використовуються ортогональні ПВП, наприклад, Уолша, кількість яких можна порівняти з базою сигналу $B_{\text{ш}}$. З усієї загальної безлічі комбінацій $N_{\text{заг}} = 2^n$ вибирається тільки $N_p = n - 1$ взаємно-ортогональних ПВП. Кодова відстань між будь-якою парою послідовності Уолша на відміну від циклічних кодів відповідає фіксованому значенню:

$$d_0 = \frac{n}{2}, \quad (1.64)$$

що забезпечує здатність виявлення до $t_0 = d_0 - 1$ помилок. Теоретично це означає, що при кореляційному прийомі правильне розпізнавання ПВП можливе за умови, що кількість спотворених бітів t_0^* не перевищує половини довжини послідовності, тобто $t_0^* \leq n/2$. Виявлення сигналу засобами РЕР свідчить про подолання рівня захисту каналу на фізичному рівні, тобто про порушення умов енергетичної прихованості. У разі реалізації другого сценарію протидії, спрямованого на розкриття змісту перехопленого повідомлення, необхідним є попереднє розпізнавання структури сигнальних конструкцій. Структурна прихованість визначається кількістю двійкових вимірювань (бітів інформації), які необхідно виконати для встановлення структури сигналу:

$$S = \log_2 A, \quad (1.65)$$

де A – потужність ансамблю реалізацій, що визначається кількістю усіх можливих комбінацій параметрів сигнально-кової конструкції.

До таких параметрів належать: несуча частота, тип модуляції, структура кодування, час надходження сигналу, фазові та частотні зсуви тощо. Отже, структурна прихованість тісно пов'язана з методами побудови сигнальної структури: чим більше змінних параметрів у сигнально-кових конструкціях, тим вищий ступінь їхньої прихованості. Для підвищення структурної прихованості передавач має формувати максимально широкий ансамбль сигналів зі змінними в часі характеристиками. Збільшення кількості реалізацій можливе, зокрема, шляхом використання складніших видів модуляції, таких як BPSK (ФМ-2), 4-QAM, 8-QAM, 16-QAM, 32-QAM тощо. На рис. 1.10 представлена залежність структурної прихованості від ступеня позиційності сигнально-кових конструкцій M .

Вочевидь, що підвищення структурної прихованості за рахунок ускладнення сигнальних конструкцій призводить до перерозподілу ресурсів каналу зв'язку. Перехід до багатопозиційних систем модуляції покращує частотну ефективність:

$$\gamma = \frac{R}{\Delta F}, \quad (1.66)$$

однак супроводжується зниженням енергетичної ефективності:

$$\beta = \frac{R}{h_0^2}, \quad (1.67)$$

де R – швидкість передавання інформації, $h_0^2 = P_s/N_0$ – відношення середньої потужності сигналу до спектральної щільності адитивного білого гаусового шуму N_0 .

Для оцінки впливу перерозподілу ресурсів на завадостійкість і структурну прихованість було проведено імітаційне моделювання сигналів типу BPSK, 8-QAM,

16-QAM, 32-QAM у каналі з АБГШ. Результати, представлені на рис. 1.11, демонструють залежність імовірності помилки на біт p_0 від відношення сигнал/шум h_0^2 .

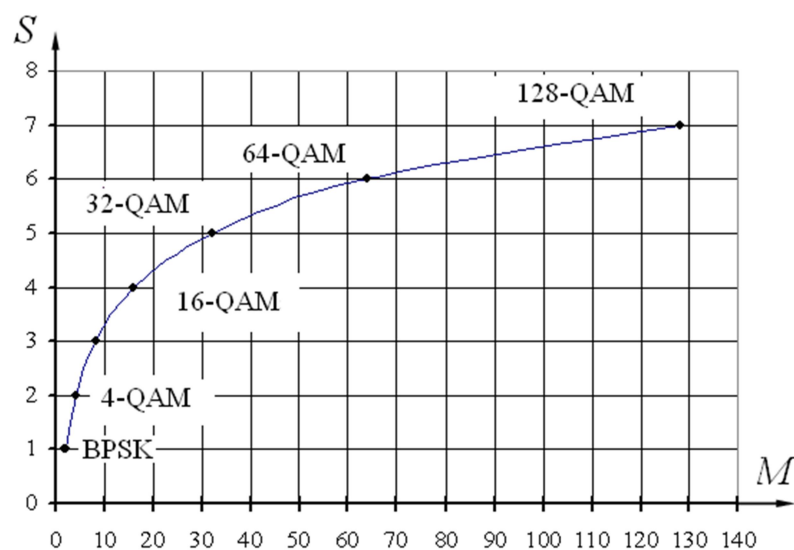


Рисунок 1.10 – Залежність структурної прихованості видів модуляції від M

Аналіз результатів показав, що складніші види модуляції забезпечують вищу швидкість передавання, однак зменшують завадостійкість сигналу. Водночас багатопозиційні модуляції сприяють зростанню структурної прихованості сигнальних конструкцій за рахунок збільшення ансамблю реалізацій.

Подальше підвищення структурної прихованості можливе шляхом ускладнення форми модулюючого сигналу. У цьому контексті доцільно застосовувати таймерні сигнальні конструкції, які поєднуються з методами модуляції та розширення спектра. Зазвичай захищеність на основі енергетичної прихованості реалізується саме через розширення спектра вихідного сигналу, що, як уже зазначалося, веде до зниження частотної ефективності каналу. Вочевидь, що взаємозалежність між показниками енергетичної та частотної ефективності каналу створює можливість для оптимізації процесу підвищення енергетичної прихованості сигнальних конструкцій. Крім того, застосування широкосмугових сигналів сприяє покращенню електромагнітної сумісності систем радіозв'язку з іншими передавальними пристроями.

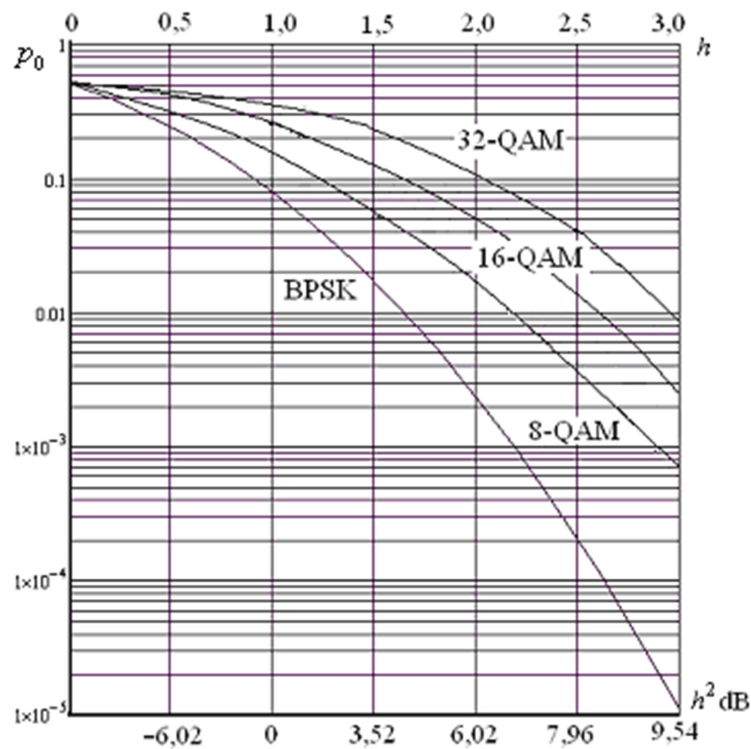


Рисунок 1.11 – Залежності ймовірності помилок систем з BPSK, 8-QAM, 16-QAM, 32-QAM від h_0^2

Узагальнена модель оцінювання захищеності методів передавання інформації передбачає кількісне оцінювання рівня захищеності у завадозахищених інформаційно-комунікаційних системах на основі системи показників, яка враховує витрати енергетичних, частотних та інформаційних ресурсів каналу зв'язку, зокрема за такими критеріями:

1) максимальна енергетична прихованість досягається у того методу передавання, який за заданої смуги широкосмугового сигналу ΔF та необхідного рівня достовірності забезпечує мінімальне відношення сигнал/шум h_0^2 :

$$\min h_0^2 = E\{\Delta F; P_{\text{НП}}(n)\}, \quad (1.68)$$

де $P_{\text{НП}}(n)$ – ймовірність невиявленої помилки в кодовому блоці довжини n , $E\{\cdot\}$ – позначає функціональну залежність рівня прихованості від параметрів:

2) максимальна структурна прихованість досягається у того методу формування сигнальних конструкцій, який протягом заданого інтервалу

побудови сигналу $T_{СК}$ та при забезпеченні необхідної достовірності дозволяє сформувати найбільший ансамбль реалізацій A :

$$\max A = S\{T_{СК}; P_{НП}(n)\}. \quad (1.69)$$

Формули (1.68) та (1.69) свідчать, що суттєвий потенціал зростання прихованості радіотехнічних об'єктів досягається шляхом комбінування параметрів сигналів у частотно-часовому просторі, що дозволяє застосовувати спектральні методи захисту інформації з використанням складних сигнально-кодових конструкцій і великих баз широкосмугових сигналів $B_{ш}$. Запропонована модель дозволяє здійснювати порівняльний аналіз методів захисту за критеріями прихованості та завадостійкості з урахуванням витрат каналних ресурсів, що є ключовим для побудови ефективних захищених каналів зв'язку в умовах радіоелектронної протидії.

1.6. Розвиток методів підвищення прихованості та завадостійкості сигнальних конструкцій в умовах радіоелектронного протиборства

У сучасних умовах радіоелектронного протистояння [13, 14] одним із ключових завдань для інформаційно-комунікаційних систем спеціального призначення є забезпечення високого рівня прихованості передавання сигналів [2, 3]. Розвиток засобів радіотехнічної розвідки та електронного придушення обумовлює потребу у використанні сигнальних конструкцій, здатних залишатися непомітними в спектрі та мінімізувати ймовірність виявлення, ідентифікації або перехоплення. Подальше підвищення прихованості сигналів можливе шляхом комплексної оптимізації параметрів сигнальних конструкцій, алгоритмів їх генерації та способів адаптивного перетворення відповідно до динамічних умов середовища РЕБ. На рис. 1.12 представлено узагальнену схему підходу до вдосконалення методів прихованого передавання інформації в радіоканалах. Основні етапи цього підходу включають:

1) формування вихідних вимог до прихованості, які базуються на оцінці рівня загроз, типових сценаріях РЕБ, характеристиках противника та призначенні системи зв'язку. Це дозволяє визначити необхідні рівні енергетичної, структурної та інформаційної прихованості;

2) формальний опис сигнальних конструкцій, що відповідають заданим критеріям прихованості. До таких конструкцій належать сигнали з шумоподібною структурою, широкосмуговим спектром, хаотичними або псевдовипадковими параметрами. Визначаються характеристики спектра, кореляційних властивостей, енергетичного розподілу, часової структури тощо;

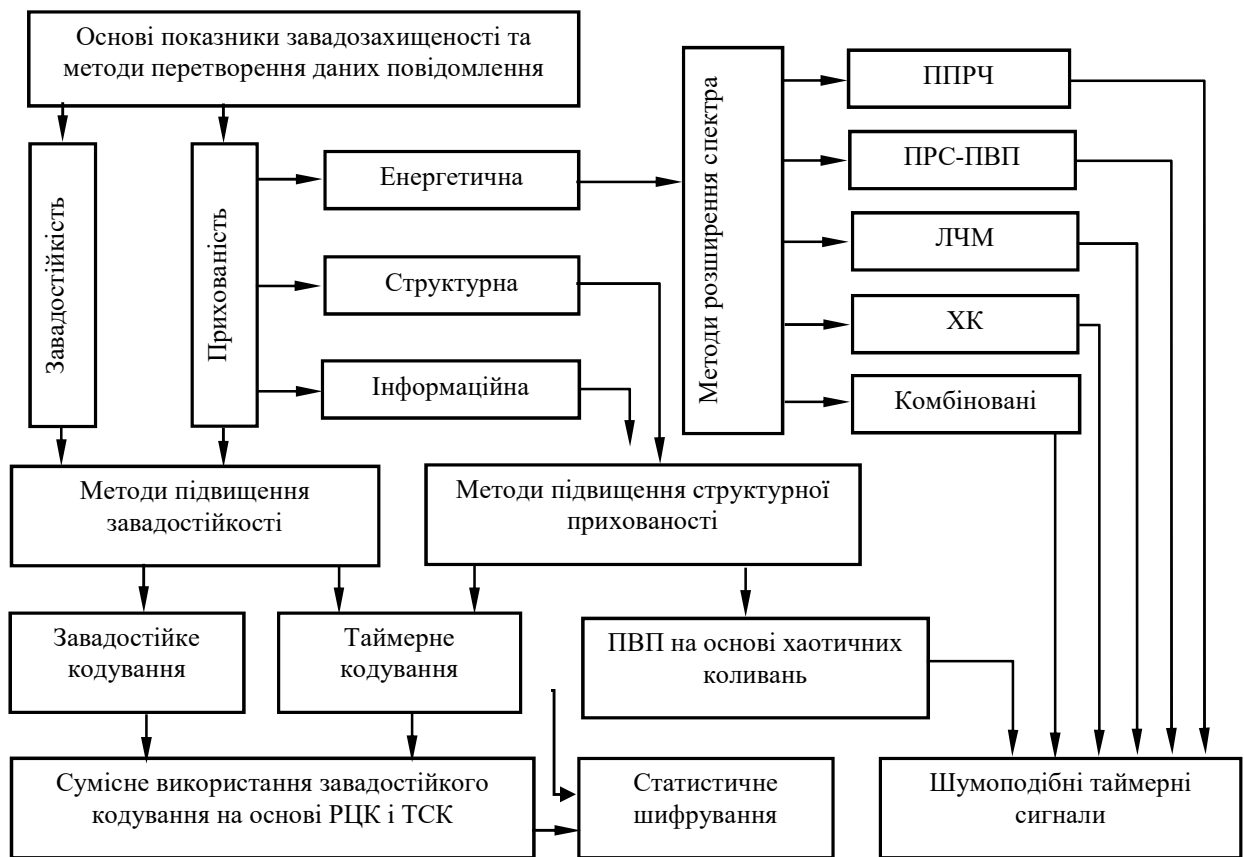


Рисунок 1.12 – Узагальнена модель вдосконалення методів прихованого передавання інформації

3) аналіз протидіючих впливів з боку засобів РЕР і РЕБ, з урахуванням потенційних каналів компрометації: виявлення, класифікація, перехоплення, аналіз протоколів, придушення або імітація. Це дозволяє адаптувати методи прихованості до конкретних типів загроз;

4) оптимізація параметрів сигнальної конструкції з урахуванням обмежень на ресурси каналу зв'язку, вимог до швидкості передавання, допустимого рівня помилок і завадостійкості. Формується задача багатокритеріальної оптимізації, де враховуються компроміси між прихованістю, енергетичною ефективністю та якістю передавання;

5) розробка адаптивних методів управління передаванням, що дозволяють змінювати структуру сигналу, схеми кодування або модуляції у відповідь на зміни у середовищі РЕБ. Це забезпечує стійкість до широкого спектра атак, включаючи інтелектуальні засоби виявлення та завад;

6) інтеграція результатів у загальну архітектуру системи зв'язку, із можливістю поєднання різнорівневих засобів захисту (від фізичного до прикладного рівня), реалізації принципів багаторівневої прихованості та забезпечення комплексної завадозахищеності.

Таким чином, перспективи підвищення прихованості передавання інформації полягають у переході від статичних схем формування сигналу до динамічних, адаптивних методів, здатних оперативно реагувати на зміни у середовищі противника. Це дозволяє створювати гнучкі, малопомітні канали зв'язку, які залишаються ефективними навіть у складних умовах електромагнітного протиборства.

1.7. Постановка задач на дослідження

Забезпечення ефективного захисту інформації в сучасних ІКС, що функціонують в умовах агресивного інформаційного середовища, є складною і постійно актуалізованою науково-технічною проблемою. Існуючі методи, такі як класичне шифрування, модулювання та алгоритми розширення спектра, орієнтовані переважно на позиційні сигнали зі сталою тривалістю елементів коду, дедалі частіше виявляються вразливими до новітніх засобів НСД і систем перехоплення сигналів. Подальше вдосконалення механізмів захисту ІКС вимагає впровадження нових сигнально-кодових конструкцій із підвищеним

рівнем структурної та енергетичної прихованості. Особливо перспективними є непозиційні сигнали, зокрема таймерні та хаотичні, що формуються за заздалегідь визначеними або псевдовипадковими алгоритмами. Використання таймерного кодування дозволяє формувати велику кількість сигнальних ансамблів зі складною структурою, підвищуючи тим самим захист від аналізу та виявлення. На основі таймерного кодування можлива реалізація інтегрованих методів захисту, які поєднують статистичне шифрування, завадостійке кодування та декореляцію помилок у єдиний процес перетворення даних. Це відкриває шлях до реалізації багаторівневих систем захисту, де кожен рівень забезпечує свою функцію: маскування сигналу, виправлення помилок, шифрування або адаптацію до параметрів каналу. Окрему увагу заслуговує застосування динамічного хаосу. Його властивості – непередбачуваність, чутливість до початкових умов, складна динаміка – дозволяють створювати високоефективні механізми шифрування та маскування інформації. Поєднання таймерних сигналів з хаотичними коливаннями дає змогу сформувати шумоподібні сигнали з високим рівнем енергетичної та структурної прихованості. Подальший розвиток теорії захисту ІКС передбачає формування узагальненої моделі оцінювання рівня завадозахищеності на основі інтеграції ключових показників: завадостійкості, енергетичної, структурної та інформаційної прихованості. Така модель повинна враховувати обмеження енергетичних, частотних та інформаційних ресурсів каналу зв'язку. Важливим напрямом є також адаптація параметрів передачі сигнально-кодових конструкцій до умов нестаціонарного середовища функціонування, зокрема при реалізації радіoeлектронного протидіювання.

Реалізація синтезу шумоподібних сигналів на основі таймерних сигналів із застосуванням методів спектрального розширення, таких як ППРЧ, ПРС-ПВП і ЛЧМ, дозволяє досягти високої енергетичної прихованості. Розробка відповідних алгоритмів вибору параметрів та методів оцінки структурної прихованості є важливою складовою побудови ефективної системи захисту.

Отже, виникає наукова проблема розробки ефективних методів

формування сигнально-кодових конструкцій та алгоритмів передавання інформації, орієнтованих на підвищення рівня прихованості та завадостійкості функціонування ІКС в умовах радіоелектронного протиборства. Вирішення зазначеної науково-практичної проблеми передбачає розв'язання комплексу взаємопов'язаних наукових задач:

1. Розробити узагальнену модель захисту інформації в інформаційно-комунікаційних системах на основі інтегральних показників завадозахищеності, зокрема – завадостійкості та різновидів прихованості (енергетичної, структурної, інформаційної). У процесі моделювання передбачається врахування обмежень енергетичних, частотних та інформаційних ресурсів каналу зв'язку, а також граничних умов його функціонування. На основі побудованої моделі провести кількісну оцінку рівня захисту від несанкціонованого доступу, а також проаналізувати ефективність застосування позиційних та непозиційних сигналів при формуванні шумоподібних сигнально-кодових конструкцій у рамках комбінованих методів захисту, що базуються на стохастичному шифруванні, завадостійкому та таймерному кодуванні.

2. Провести оцінку ефективності спільного використання таймерних і позиційних кодів для адаптації параметрів сигнально-кодових конструкцій до змін у характеристиках каналу зв'язку, зокрема в умовах його нестаціонарності. Розробити критерії адаптації до мінливих завадових умов.

3. Дослідити можливості підвищення рівня структурної прихованості та завадостійкості шляхом варіювання параметрів таймерного кодування. Особливу увагу приділити ролі базового параметра Δ , що визначає часову структуру сигналу, та встановити залежності між його значенням і рівнем захищеності. Провести аналіз здатності таймерного кодування до виявлення та корекції помилок у сигнально-кодових конструкціях.

4. Розробити концепцію багаторівневої системи захисту інформації, яка поєднує стохастичне шифрування, завадостійке та таймерне кодування. Запропонувати механізми підвищення рівня прихованості шляхом компенсації

надлишковості, що виникає під час генерації випадкових шифрограм, із залученням методів ефективного таймерного структурування сигналу.

5. Сформулювати та дослідити методи генерації шумоподібних сигналів на основі таймерних сигнальних конструкцій. Визначити критерії вибору параметрів таких сигналів з урахуванням складності їх реалізації, вимог до завадостійкості, а також рівня прихованості. Дослідити вплив параметрів таймерного сигналу на потужність множини можливих реалізацій сигнально-кодових конструкцій.

6. Провести аналіз підходів до синтезу шумоподібних сигналів із використанням таймерних конструкцій у поєднанні з методами спектрального розширення: ППРЧ, ПРС, ЛЧМ. Обґрунтувати умови досягнення енергетичної прихованості, розробити відповідні алгоритми розширення спектра та методик оцінювання рівня структурної прихованості сформованих сигналів.

Сукупне розв'язання сформульованих задач спрямоване на вирішення актуальної наукової проблеми, що має істотне значення як для розвитку теорії прихованості та завадозахищеності, так і для практичного забезпечення необхідного рівня прихованості передавання інформації в ІКС на каналному та фізичному рівнях еталонної моделі OSI.

Висновки

У першому розділі дисертаційної роботи проведено всебічний аналіз сучасного стану проблеми забезпечення захищеності ІКС в умовах активного застосування засобів РЕБ. Основні результати цього етапу дослідження полягають у наступному:

1. Сформульовано концептуальні основи побудови багаторівневого захисту ІКС на основі поєднання енергетичної, структурної та інформаційної прихованості. Обґрунтовано необхідність інтеграції засобів маскування та криптографічного захисту на фізичному та каналному рівнях моделі OSI.

2. Визначено ключові параметри сигналів, що впливають на завадозахищеність систем зв'язку: спектральна щільність потужності, тривалість, ширина спектра, динамічний діапазон, ентропія структури. На основі цих параметрів запропоновано модель обсягу сигналу як інтегральної метрики для оцінювання захищеності передачі.

3. Досліджено та систематизовано методи спектрального розширення сигналів (ПРС, ППРЧ, ЛЧМ), які забезпечують зниження спектральної помітності сигналу й ускладнюють його виявлення засобами РЕР. Встановлено, що оптимізація бази сигналу дозволяє збалансувати вимоги до завадостійкості, прихованості та апаратних ресурсів.

4. Показано ефективність використання параметричних перетворень сигнально-кодкових конструкцій для реалізації адаптивної стратегії захисту, зокрема шляхом варіативної модуляції, перестановок, стохастичних деформацій часових інтервалів.

5. Обґрунтовано взаємозв'язок між показниками завадостійкості, енергетичної прихованості та пропускною здатністю каналу, з урахуванням теореми Шеннона. Показано, що реалізація захисту з використанням широкосмугових сигналів і завадостійкого кодування дозволяє досягти високої достовірності передачі при зниженій помітності сигналу.

6. Запропоновано формалізовану систему оцінювання ефективності методів захисту інформації, яка базується на поєднанні кількісних метрик (обсяг сигналу, ентропія, база сигналу) та сценаріїв РЕБ-протидії. Це створює підґрунтя для подальшої побудови моделі вибору оптимальної сигнально-кової конструкції залежно від характеру загроз.

Узагальнюючи, у розділі сформульовано науково-прикладну проблему забезпечення прихованого та завадостійкого передавання інформації в умовах активного радіоелектронного впливу, обґрунтовано напрями подальших досліджень, пов'язані з розробкою інтегрованих методів побудови сигнально-кодкових конструкцій із властивостями багаторівневої прихованості та адаптивної завадозахищеності.

2 ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПЕРЕДАВАННЯ ДАНИХ НА ОСНОВІ СУМІСНОГО ВИКОРИСТАННЯ БЛОКОВИХ ЗАВАДОСТІЙКИХ КОДІВ ТА ТАЙМЕРНИХ СИГНАЛІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У розділі розглянуто підходи щодо захисту інформації на основі підвищення завадостійкості та ефективності передавання повідомлень в умовах нестаціонарного каналу зв'язку. Проведено моделювання каналу за допомогою моделі Елліота–Гільберта, яка враховує наявність «хороших» і «поганих» станів. Проаналізовано вплив параметрів завадостійкого кодування на якість і швидкість передачі, а також обґрунтовано можливість трансформації запасу завадостійкості у збільшення швидкості передавання. Особливу увагу приділено використанню таймерних сигнальних конструкцій у поєднанні з блоковими кодами для забезпечення адаптивного управління передачею даних залежно від стану каналу. Показано переваги такого підходу при захисті інформації в умовах радіоелектронного впливу.

2.1. Огляд математичних моделей дискретного каналу з точки зору придатності до умов РЕБ

Для забезпечення надійності та захищеності передавання даних в умовах дії засобів РЕБ [12, 13] особливе значення має вибір адекватної математичної моделі каналу зв'язку. Метою моделювання є опис характеру передавання сигнальних конструкцій, динаміки змін параметрів каналу, впливу завад та можливостей для адаптації сигнально-кодових конструкцій. Найбільш простою математичною моделлю дискретного каналу є класична біноміальна модель каналу з незалежними помилками [50, 51]. В цій моделі передача кожного біта здійснюється з ймовірністю помилки p_0 , яка є сталою та незалежною від часу. Вона дозволяє отримати базову оцінку ефективності каналів та кодування, хоча

не враховує корельованості помилок або імпульсного характеру завад, що характерно для каналів у умовах РЕБ. Розглянемо ймовірність помилки одиничного біта. Нехай $X \in \{0, 1\}$ - переданий біт, $Y \in \{0, 1\}$ – отриманий біт. Тоді ймовірність помилкового прийому описується формулою:

$$P_r(Y \neq X) = p_0, \quad P_r(Y = X) = p_0. \quad (2.1)$$

Розглянемо ймовірність помилки кодової комбінації. Нехай кодова комбінація складається з n бітів, і всі біти передаються незалежно. Тоді ймовірність того, що у комбінації буде принаймні одна помилка, обчислюється як [51]:

$$P(1, n) = 1 - (1 - p_0)^n. \quad (2.2)$$

Ця формула демонструє, що навіть при невеликій ймовірності помилки одного біта p_0 , ймовірність помилки всієї кодової комбінації зростає зі збільшенням довжини n . Ймовірність того, що рівно k бітів з n будуть помилковими, то вона описується біноміальним розподілом [50]:

$$P(k, n) = \binom{n}{k} p_0^k (1 - p_0)^{n-k}, \quad k = 0, 1, 2, \dots, n, \quad (2.3)$$

де $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ – біноміальний коефіцієнт. З цієї формули можна отримати середню кількість помилок у комбінації:

$$E[K] = n \cdot p_0, \quad (2.4)$$

де K – випадкова величина, що позначає кількість помилок у комбінації. Ця модель не враховує корельованості помилок, характерної для імпульсних або групових завад, які характерні для систем зв'язку, що працюють в умовах РЕБ.

Крім цього, ця модель не описує часові зміни якості каналу, які спостерігаються при дії засобів глушіння сигналу засобами РЕБ. Отже, біноміальна модель каналу з незалежними помилками є простим і наочним інструментом для початкового аналізу ефективності систем передачі. Вона добре підходить для оцінки базових характеристик дискретного каналу та середньої кількості помилок, але для більш реалістичного моделювання каналів у умовах РЕБ необхідно використовувати моделі з корельованими помилками, такі як марковські моделі (Гілберт–Елліот) або модель Пуртова.

Модель Пуртова [50] є однією з найбільш зручних для аналітичного опису дискретного каналу з групуванням помилок. На відміну від класичної біноміальної моделі, де всі помилки вважаються незалежними, дана модель враховує факт, що в реальних каналах зв'язку під впливом завад (зокрема імпульсних та корельованих) помилки схильні до кластеризації, тобто виникають не поодинокі, а серіями. Ймовірність спотворення кодової комбінації довжини n у моделі Пуртова визначається виразом [51]:

$$P(\geq 1; n) = p_o n^{1-\alpha}, \quad (2.5)$$

де: α – коефіцієнт групування помилок, що відображає рівень їхньої корельованості.

Можна відзначити, що при $\alpha=1$ формула (2.5) вироджується у класичну біноміальну модель незалежних помилок, де ймовірність зростає лінійно з довжиною комбінації [50]:

$$P(\geq 1; n) = p_o n. \quad (2.6)$$

При $0 < \alpha < 1$ відбувається посилене групування помилок, тобто зі збільшенням n ймовірність спотворення зростає повільніше, ніж у випадку незалежних помилок. У випадку, коли $\alpha \rightarrow 0$ модель описує ситуацію, коли практично всі помилки зосереджені у вигляді пачок, а між ними існують довгі

ділянки без помилок. Отже, параметр α є зручним індикатором, що дозволяє описати перехід від незалежних помилок до сильно корельованих, характерних для каналів, які працюють в умовах інтенсивних завад. На рис. 2.1 наведено залежності ймовірності спотворення кодової комбінації $P(\geq 1; n)$ від коефіцієнта групування α при фіксованому значенні ймовірності бітової помилки $p_o = 5 \cdot 10^{-5}$. Ці криві наочно демонструють, що зменшення α призводить до більш повільного зростання ймовірності спотворення комбінації з ростом її довжини.

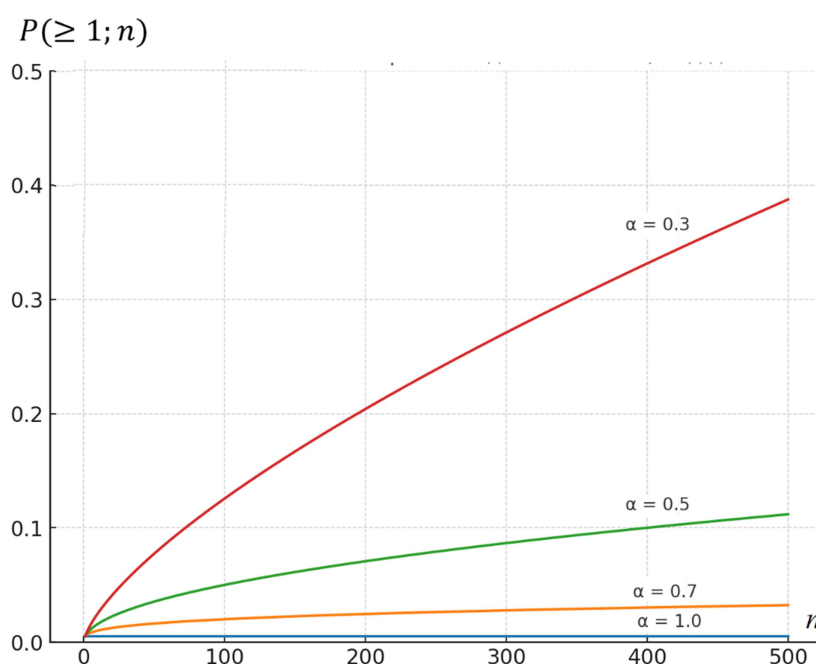


Рисунок 2.1 – Залежності ймовірності спотворення кодової комбінації $P(\geq 1; n)$ від n та α

Можна відзначити, що модель Пуртова є ефективним інструментом для опису процесів передавання інформації в умовах, коли спотворення носять групований характер. На відміну від класичної біноміальної моделі з незалежними помилками, вона враховує корельованість спотворень, що суттєво підвищує адекватність опису реальних каналів зв'язку, особливо в ситуаціях інтенсивних завад. В умовах РЕБ, де формуються навмисні завадові впливи, характерними є саме групові (пакетні) помилки, що виникають у результаті

імпульсних або адаптивних завад. У таких випадках застосування моделі Пуртова дозволяє: оцінювати ймовірність спотворення кодових комбінацій із урахуванням коефіцієнта групування помилок; формалізовано описувати вплив завад на довгі та короткі кодові блоки; отримувати статистичні залежності, що відображають реальний розподіл помилок у часі. Отже, використання моделі Пуртова в дослідженнях систем зв'язку, що функціонують в умовах РЕБ, є доцільним і виправданим. Вона забезпечує більш точну оцінку завадостійкості кодів і протоколів передачі порівняно з класичними моделями незалежних помилок, дозволяє визначати вимоги до коригувальних кодів і протоколів ARQ [32, 33], а також обґрунтовувати методи оптимізації надлишковості в умовах інтенсивного завадового впливу.

Модель Гільберта описується двома станами дискретного каналу [33]: у Х-стані помилок практично не виникає; у П-стані помилки з'являються з ймовірністю p_{Π} . Матриця перехідних ймовірностей має вигляд:

$$P = \begin{bmatrix} P_{XX} & P_{X\Pi} \\ P_{\Pi X} & P_{\Pi\Pi} \end{bmatrix}, \quad (2.7)$$

де елемент P_{xy} визначає ймовірність переходу системи в стан y на наступному кроці за умови, що на поточному кроці вона перебувала у стані x .

Оскільки матриця є стохастичною, виконується умова нормування:

$$P_{XX} + P_{X\Pi} = 1, P_{\Pi X} + P_{\Pi\Pi} = 1. \quad (2.8)$$

Граф-схему переходів станів моделі Гільберта описується ланцюгом Маркова та представлена на рис. 2.2. Ймовірності, що характеризують довготривале (стаціонарне) перебування системи у кожному з можливих станів, визначаються співвідношеннями [50, 51]:

$$P_{\Pi} = \frac{P_{X\Pi}}{P_{\Pi X} + P_{X\Pi}}; \quad P_X = \frac{P_{\Pi X}}{P_{\Pi X} + P_{X\Pi}}. \quad (2.9)$$

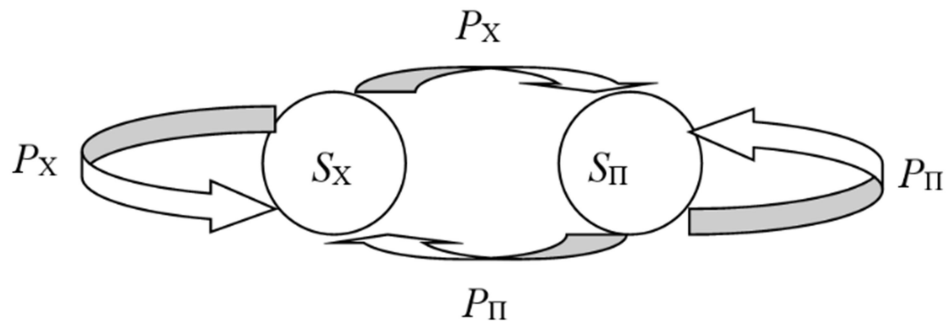


Рисунок 2.1 – Граф-схему переходів станів моделі Гільберта

Середня ймовірність помилкового прийому елемента визначається наступним чином:

$$\overline{p_n} = p_n \cdot P_П = p_n \cdot \frac{P_{XП}}{P_{ПХ} + P_{XП}}. \quad (2.10)$$

Середня тривалість «хорошого» і «поганого» станів становить [51, 52]:

$$\tilde{l}_X = \frac{1}{P_{XП}}; \quad \tilde{l}_П = \frac{1}{P_{ПХ}}. \quad (2.11)$$

Показник $\tilde{l}_X$ визначає середню довжину «безпомилкових серій», а $\tilde{l}_П$ – середню довжину «пачки помилок». Оцінка параметрів моделі можлива на основі статистики середніх довжин станів:

$$P_{XП} = \frac{1}{\tilde{l}_X}; \quad P_{ПХ} = 1 - P_{XП}; \quad P_{ПХ} = \frac{1}{\tilde{l}_П}; \quad P_{ХХ} = 1 - P_{ПХ}. \quad (2.12)$$

Отже, модель Гільберта дозволяє безпосередньо пов'язати експериментально спостережувані параметри (середні довжини серій) із характеристиками завадостійкості каналу. Це створює основу для коректного математичного моделювання каналів у системах передачі, що працюють в умовах активних завад та групування помилок. Слід відзначити, що модель Гільберта, яка базується на двостановому марковському процесі, є однією з

найбільш придатних для опису функціонування систем радіозв'язку в умовах дії навмисних завад. Її перевага полягає у можливості відображення характерного для РЕБ ефекту чергування інтервалів «нормальної» роботи каналу з низькою імовірністю помилки та інтервалів інтенсивних завад із різким зростанням рівня спотворень. Завдяки введенню параметрів середніх довжин «хорошого» та «поганого» станів дозволяє адекватно описувати статистику появи помилок у вигляді кластерів, що є типовим для каналів, зазнаних впливу засобів радіоелектронної боротьби. Це робить її більш точною в порівнянні з класичними моделями з незалежними помилками та дозволяє коректно оцінювати ефективність корекційних кодів, протоколів ARQ і комбінованих методів захисту інформації. Отже, модель Гільберта є ефективним інструментом для аналізу і моделювання завадостійкості систем радіозв'язку в умовах РЕБ, оскільки відображає реальні статистичні характеристики помилок і забезпечує основу для розробки оптимальних методів захисту інформації.

2.2. Вплив надлишковості на ефективність завадостійкого обміну даними

Досвід практичного впровадження та результати теоретичних досліджень ІКС із автоматичним запитом повторної передачі (Automatic Repeat Request – ARQ) [50, 51] свідчать, що під час організації завадостійкого обміну даними надлишковість сигналу є критичним фактором, що визначає ефективність роботи системи. Встановлено, що понад 95 % загальної надлишковості, яка припадає на передавання одного інформаційного двійкового елемента, формується саме за рахунок введення перевірних (контрольних) розрядів. Такий високий рівень надлишковості обумовлений низкою факторів, серед яких ключовими є:

- 1) необхідність застосування відносно коротких сигнальних конструкцій у високошвидкісних та високодинамічних телекомунікаційних системах.

Обмежена довжина кодових комбінацій викликана тим, що передана інформація швидко втрачає актуальність (ефект «старіння» даних), а отже, не може передаватися з використанням довгих кодових блоків. Це вимагає підвищеної насиченості перевірними розрядами;

2) наявність у реальних каналах зв'язку ефекту групування помилок, коли спотворення виникають не незалежно одне від одного, а зосереджуються у вигляді пачок (кластерів). У таких умовах класичні коди, розраховані на незалежні випадкові помилки, втрачають ефективність, що змушує застосовувати більш складні та надлишкові коди для забезпечення необхідного рівня завадостійкості.

У сукупності ці чинники зумовлюють високу частку контрольних символів у загальному обсязі переданої інформації, що, з одного боку, знижує ефективність використання каналу, але з іншого – забезпечує гарантовану достовірність обміну навіть в умовах сильних завад та інтенсивного групування помилок. Саме ця обставина обґрунтовує доцільність подальших досліджень методів оптимізації надлишковості, адаптивного використання ARQ та побудови комбінованих схем кодування і повторної передачі, орієнтованих на роботу в реальних заводських умовах.

Розглянуто можливість адаптивного обміну між якістю і швидкістю передавання залежно від поточного стану каналу. Зокрема, проаналізовано ефективність реалізації такого обміну в інтервалах «хорошого» стану каналу за допомогою таймерних сигнальних конструкцій, із подальшим відновленням якості передачі шляхом використання розрядно-цифрових кодів. Розв'язання задачі підвищення достовірності передачі в таких умовах здійснюється двома підходами: застосуванням надлишкових кодів (у системах із прямим каналом) та використанням адаптивних методів (у системах зі зворотним зв'язком). Відомі методи визначення параметрів завадостійкого коду здебільшого спрямовані на пошук оптимальної надлишковості для забезпечення заданого рівня вірності приймання. Проте навіть мінімально припустиме значення надлишковості розрядно-цифрових кодів призводить до зменшення швидкості

передавання в каналі. Проведений аналіз показує, що при виборі параметрів завадостійкого коду часто не враховується наявний запас завадостійкості у бінарних системах передавання, який притаманний реальним каналам зв'язку.

Для виконання поставленого завдання була обрана модель Елліота–Гільберта, яка описує нестаціонарний канал зв'язку у вигляді двох станів: «хорошого» та «поганого». Такий підхід є обґрунтованим з точки зору функціонування систем радіозв'язку в умовах дії засобів РЕР. У «хорошому» стані каналу ймовірність вірного приймання даних на кілька порядків перевищує середню ймовірність помилки, тоді як у «поганому» стані вона наближається до 0,5, що свідчить про повне глушіння каналу. Зазвичай канал перебуває в «хорошому» стані до 98–99% часу, тоді як «поганий» стан спостерігається лише 1–2% часу. Наприклад, при співвідношенні сигнал/шум $h \geq 10$ у «хорошому» стані, ймовірність бітової помилки становить $p_x \leq 10^{-9} \dots 10^{-8}$, що забезпечує значний запас завадостійкості відносно середнього значення помилки $\bar{p}_e$. Водночас, якщо в «поганому» стані (з питомою вагою $\gamma_{\Pi} = 0,01$) ймовірність помилки становить $p_{\Pi} = 0,5$, а в «хорошому» стані $\gamma_x = 0,99$ та $p_x < 10^{-8}$, то середня ймовірність помилки у каналі: $\bar{p}_e = \gamma_x \cdot p_x + \gamma_{\Pi} \cdot p_{\Pi} = 0,99 \cdot 10^{-8} + 0,01 \cdot 0,5 \approx 5 \cdot 10^{-3}$ визначається "поганим" станом.

При цьому вибір надлишковості коду доцільно здійснювати або з урахуванням найгіршого стану каналу, або на основі середньої ймовірності помилки в нестаціонарному середовищі. Оцінимо можливість збільшення швидкості передавання інформації в реальному каналі. Якщо алфавіт каналу має розмірність " a " станів, то на інтервалі тривалості $T_c = mt_0$ може існувати $N_p = a^m$ можливих реалізацій сигналу. З наведеного прикладу можна зробити висновок, що середня ймовірність елемента в дискретному каналі наближається до значення 5×10^{-3} і залежить від Π -стану каналу. При таких статистичних характеристиках каналу передавані сигнальні конструкції мають великий запас надійності по достовірності в X -стані каналу. Це обґрунтовує доцільність обміну достовірності передавання на швидкість, враховуючи поточний стан дискретного каналу

Збільшення кількості реалізацій сигнальних конструкцій можливе за рахунок зменшення мінімальної відстані між ЗММ у каналі з базою, що дорівнює одиниці, тобто за рахунок підвищення швидкості передавання вище класичної межі Найквіста. Прикладом такого підходу є ТСК, у яких відстань між ЗММ не менша за найквістовий інтервал $t_0 = 1/\Delta F$, однак вона не є кратною цьому інтервалу. Замість цього відстань обирається кратною деякому підінтервалу $\Delta = t_0/s$, де $(s \in 2, 3, \dots k)$. Загальна відстань між ЗММ тоді визначається як $\tau_c = t_0 + \Delta i$. Значення s вказує, наскільки зменшується інтервал Δ відносно базової тривалості t_0 . Така форма організації ЗММ дозволяє ефективно усунути міжсимвольні спотворення (МСС) при збільшенні швидкості передавання інформації, що ілюструє перевагу використання ТСК для побудови завадостійких систем зв'язку.

2.3. Обґрунтування адаптивного обміну запасу якості передавання інформації на швидкість

При використанні систем кодування на основі РЦК [33, 50] підвищення пропускної здатності каналу досягається за рахунок більш щільного розташування сигнальних точок у просторі станів модуляції. Це, у свою чергу, еквівалентно зменшенню енергетичної відстані між сусідніми сигнальними станами, що відповідають різним значенням інформаційного параметра a_k (фаза, амплітуда або частота). На інтервалі Найквіста t_0 такий процес можна формально описати співвідношенням [50]:

$$d = \sqrt{\frac{2E_s}{M}}, \quad (2.13)$$

де d – мінімальна відстань між сусідніми сигнальними станами, E_s – енергія символу, M – кількість можливих сигнальних станів (розмір алфавіту модуляції).

Кількість сигнально-кодкових комбінацій при цьому складає:

$$M = \log_2 a_k. \quad (2.14)$$

Для бінарного каналу також можливо зменшення енергетичної відстані d між дозволеними ТСК, що дозволяє збільшити кількість реалізацій на інтервалі їх побудови T_c . Вочевидь, що призводить до зростання пропускної здатності передавання інформації. Кількість дозволених реалізацій ТСК з i -фронтами дорівнює [50]:

$$N_p = C_{ms-i(s-1)}^i \times (a_k - 1)^i. \quad (2.15)$$

Максимальна кількість інформації, що передається при цьому складає [52]:

$$J_{\max} = \log_2 C_{ms-i(s-1)}^i + i \log_2 (a_k - 1), \quad (2.16)$$

де $i = 1, \dots, m$ – кількість ЗММ.

При значенні $a_k=2$ права частина виразу (2.16) буде дорівнювати нулю і перетворюється у вираз (2.14). Сумарна кількість реалізацій $N_{p\Sigma}$ складає [51]:

$$N_{p\Sigma} = \sum_{i=1}^m C_{ms-(s-1)}^i. \quad (2.17)$$

Пропускна здатність дискретного каналу без пам'яті оцінюється за формулою [50, 51]:

$$C = \frac{1}{m} (\log_2 N_{p\Sigma} - H_b), \quad (2.18)$$

де: $\log_2 N_{p\Sigma} = H_{max}$ – максимальне значення інформації без втрат, що передається сигнальними конструкціями, побудованих на інтервалі часу T_c ; H_b – втрати інформації через спотворення сигнальних конструкцій в приймачі.

Рівень втрат інформації в каналі із завадами впливає на пропускну здатність [51]:

$$H_b \leq (1 - P_n) \log_2(1 - P_n) + P_n \log_2 \frac{P_n}{N_p - 1}. \quad (2.19)$$

де: P_n – імовірність прийняття помилкового рішення про прийом сигнальної конструкції. Імовірності помилкового і вірного прийому сигнальних конструкцій при використанні множини з числом відрізків від 1 до m визначаються як [50]:

$$P_n = 1 - \left[2\Phi\left(2h/S\right) \right]^i, \quad (2.20)$$

$$P_b = 1 - P_n, \quad (2.21)$$

де $\Phi\left(2h/S\right)$ – функція Крампа.

Для каналу з двома станами («хороший» та «плохий») загальна пропускну здатність розраховується з урахуванням показників питомої ваги кожного із них [52]:

$$\bar{C} = \gamma_x C_x + \gamma_n C_n. \quad (2.22)$$

Залежності значень $\bar{C}$ від h при $m = 5$, $i = 3$ та $s = 5, 7, 9$ представлені на рис. 2.3. Бачимо, що в реальних каналах зв'язку в "хорошому" стані каналу ($h \geq 10$) пропускну здатність системи зв'язку з ТСК більше ніж в 2 рази в

порівнянні з РЦК. Це обґрунтовує доцільність використання ТСК для підвищення швидкості передавання інформації в «хорошому» стані каналу.

Розглянемо можливість перетворення надлишку пропускної здатності на підвищення якості передачі за умови, що імовірність перебування каналу у «хорошому» стані становить $p_x < 0,99 \cdot 10^{-8}$, а у «поганому» – $p_x = 0,5$. Для порівняння розглянемо дві системи передавання:

1) двійковий код Хеммінга з параметрами: $m = 5$ інформаційних бітів, $r = 4$ перевірочних бітів, $n = 9$ загальна довжина кодового слова, $N_{p\text{ рцк}} = 512$, режим виправлення однократних помилок ($t_b = 1$);

2) таймерний сигнал, який забезпечує $N_{p\text{ тск}} = 680$ реалізацій на інтервалі $5t_0$ при $i = 3, s = 7$.

Розрахунок параметрів для РЦК були виконані для середньої ймовірності помилки $\bar{p} = 5 \cdot 10^{-3}$ і коефіцієнта групування $\alpha = 0,32$. Відносна ефективна швидкість передавання R наведена у табл. 2.1. Ймовірність помилки в кодовому блоку для РЦК:

$$P_{\Pi} = P(\geq 1, n) = \bar{p} \cdot n^{1-\alpha}, \quad (2.23)$$

або з урахуванням виправлення однократної помилки:

$$P(\geq 2, n) = \bar{p} \cdot (n/2)^{1-\alpha}. \quad (2.24)$$

Для ТСК з урахуванням того, що $2h/s = \Delta/2\sigma$ формула (2.20) перетворюється в наступний вираз [51]:

$$P_{\Pi} = 1 - \left[2\Phi\left(\frac{\Delta}{2\sigma}\right) \right]^i. \quad (2.25)$$

При $s = 7$ для «хорошого» стану каналу використовується відповідне середньоквадратичне відхилення фронту ЗММ фронту сигнальної конструкції $\sigma = 0,0178t_0$. Аналіз прикладу показує, що ТСК дозволяють отримати у 1,32 раза більше реалізацій на інтервалі $5t_0$, ніж РЦК. При цьому передача ТСК здійснюється за час, у 1,8 раза коротший, ніж для РЦК. Це означає, що протягом одного і того самого інтервалу часу T_i можливо передати більшу кількість сигнальних конструкцій, ніж при використанні РЦК. Якщо припустити, що кількість помилок у каналі на інтервалі T_i залишається сталою, тоді за рахунок збільшення кількості переданих конструкцій імовірність помилки для ТСК зменшується. Проведені розрахунки підтверджують це: ймовірність помилки при використанні ТСК є нижчою, ніж у РЦК навіть з виправленням однократних помилок (табл. 2.1).

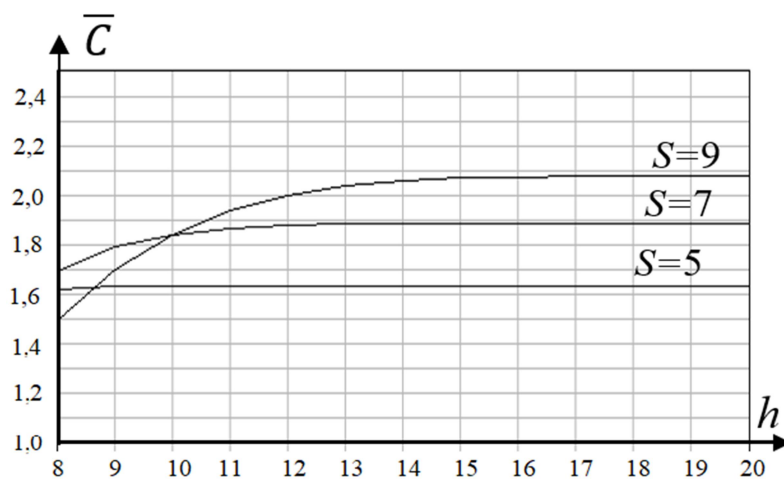


Рисунок 2.3 – Залежності $\bar{C}$ від h при параметрах ТСК $m = 5$, $i = 3$ та $s = 5, 7, 9$

Це означає, що в умовах «хорошого» стану каналу можливо передавати значно більший обсяг інформації за допомогою ТСК, ніж при використанні РЦК. Частину приросту відносної швидкості передачі можна використати для підвищення завадостійкості системи шляхом застосування кодів, здатних виправляти помилки. Отже, у бінарній системі зв'язку існує можливість трансформувати запас завадостійкості у збільшення швидкості передавання без

втрати якості приймання кодових блоків, завдяки використанню оптимальних структур сигнальних конструкцій.

Таблиця 2.1 – Розрахункові значення параметрів системи передавання, що використовує ТСК та РЦК

№	Параметри кодових комбінацій	N_p	R	P_{π}
1	РЦК ($n = 9, m = 5$)	512	0,55	$2,2 \times 10^{-2}$
2	РЦК ($n = 9, m = 5, t_B = 1$)			$1,4 \times 10^{-2}$
3	ТСК ($n = 12, m = 5, s = 7$)	680	1,88	$1,79 \times 10^{-4}$
4	РЦК ($n = 9, r = 4, t_B = 1$) сумісно з ТСК ($m = 5, i = 3, s = 7$)	680	1,05	$1,12 \times 10^{-4}$

2.4. Кореляційна залежність міжсимвольних завад та інформаційних сигналів

Для реальних каналів зв'язку характерним є ряд властивостей, які призводять до суттєвого спотворення передаваних сигнальних конструкцій. Це може бути флуктуаційна завада, тремтіння фази, імпульсна завада, короткочасна змінами рівня, спотворення АЧХ та ФЧХ та іншими. Дослідження показали [55], що значний вплив на рівень спотворення дискретних сигналів при їх передачі по каналу зв'язку вносять короткочасні впливи, до яких відносяться імпульсні завади і скачки рівня. Це справедливо по відношенню до ІКС, що працюють при питомих швидкостях 1...3 біт/с Гц і більше. При цьому відчутний вплив на якість передавання починають відігравати спотворення АЧХ і ФЧХ. Як правило, ці спотворення призводять до зміни форми передаваних сигналів, що спричиняє появу в них так званих «хвостів», які тягнуться за сигналами-переносниками. Також спостерігається інтерференція з наступними сигналами-переносниками. Отже, виникає явище міжсимвольної інтерференції. За умови, що стрибки рівня сигналу та імпульсні завади

виникають порівняно рідко й порушують лише незначну частину сигналу (що є прийнятним для більшості практичних ситуацій), вплив спотворень, зумовлених передатною функцією каналу, може розглядатися як стаціонарний. Водночас, якщо рівень міжсимвольної завади перевищує допустиме значення, це призводить до зниження достовірності передавання інформації нижче встановленого порогу протягом усього сеансу зв'язку.

Практика експлуатації ІКС апаратури свідчить, що основним джерелом помилок у каналах зв'язку є міжсимвольна інтерференція, зумовлена спотворенням передавальної функції каналу. У зв'язку з цим, першочергова увага повинна приділятися методам протидії двом основним факторам, що діють одночасно та постійно: міжсимвольній інтерференції та флуктуаційним завадам. Для аналізу розглянемо спрощену структурну схему передавання дискретної інформації з використанням амплітудно-імпульсної модуляції (АІМ), зображену на рис. 2.4. У процесі модуляції формуючий фільтр $\Phi_{\text{пер}}$ збуджується послідовністю δ -імпульсів, що надходять з інтервалом часу, який дорівнює тактовому періоду t_0 . Кожен δ -імпульс попередньо модулюється множенням на інформаційний параметр a_k , який випадковим чином набуває, наприклад, двох можливих значень: $+1$ і -1 відповідно до полярності імпульсів, що генеруються джерелом даних. Формуючий фільтр $\Phi_{\text{пер}}$, який характеризується передатною функцією $F_{\text{пер}}(\omega)$, здійснює перетворення вхідного сигналу [55]:

$$x_{\text{вх}} = \sum_{k=-\infty}^{\infty} a_k \delta(t - kt_0) \quad (2.26)$$

у модульований сигнал:

$$x_{\text{м}} = \sum_{k=-\infty}^{\infty} a_k f_{\text{пер}}(t - kt_0), \quad (2.27)$$

де: $f_{\text{пер}}(t) = \frac{1}{2\pi} \int_{-\Omega}^{\Omega} F_{\text{пер}}(\omega) e^{i\omega t} d\omega$ – імпульсна реакція формуючого фільтру.

Сигнал $x_{\text{м}}$ є придатним для подальшої передачі каналом зв'язку. Сигнал $x_{\text{м}}$ з

$$Q(\omega) = F_{\text{пер}}(\omega)G(\omega)F_{\text{пр}}(\omega). \quad (2.28)$$

Нехай імпульсна характеристика загального тракту:

$$q(t) = \int_{-\infty}^{\infty} Q(\omega)e^{i\omega t}d\omega \quad (2.29)$$

Якщо для моментів часу $t = lt_0, l = 0, \pm 1, \dots$ виконується умова, що

$$q(kt_0) = \begin{cases} 1, k = 0 \\ 0, k \neq 0 \end{cases} \quad (2.30)$$

При цьому стробування сигналу на виході приймального фільтра описується рівнянням

$$a = \sum_{k=-\infty}^{\infty} a_k q(t - kt_0) \quad (2.31)$$

у моменти часу $t = lt_0, l = 0, \pm 1, \dots$, що дозволяє точно відновлювати значення інформаційних параметрів $a_k, \dots, k = 0, \pm 1, \dots$. Дійсно, для довільного моменту часу $t = lt_0$, згідно з умовою (2.30), виконується:

$$q(lT - kt_0) = \begin{cases} 1, k = l, \\ 0, k \neq l. \end{cases} \quad (2.32)$$

тому вихідний сигнал при $t = lt_0$ дорівнює a_l для будь-якого цілого l .

Однак, якщо умова (2.30) не виконується і імпульсна реакція $q(t)$ має ненульові значення ще хоча б у одній відліковій точці $t = lt_0$ (крім $t = 0$, як показано на рис. 2.5 для $l = 0$, то при стробуванні сигналу (2.31) у момент $t = 0$ на виході ключової схеми отримаємо [40]:

$$\sum_{k=-\infty}^{\infty} a_k q(t - kt_0)|_{t=0} = a_0 + a_{-l}q(lt_0). \quad (2.33)$$

Тут a_0 є корисним сигналом, а доданок $a_{-l}q(lt_0)$ відповідає заваді, зумовленій попередніми символами, які передували прийнятому. Таку заваду

називають міжсимвольною інтерференцією. Вона виникає внаслідок дії переданого сигналу на спотворюючий канал і за відсутності сигналу зникає. При цьому спотворення, зумовлені фазо-частотною характеристикою каналу, подовжують «хвіст» імпульсної реакції, що й призводить до появи міжсимвольного впливу.

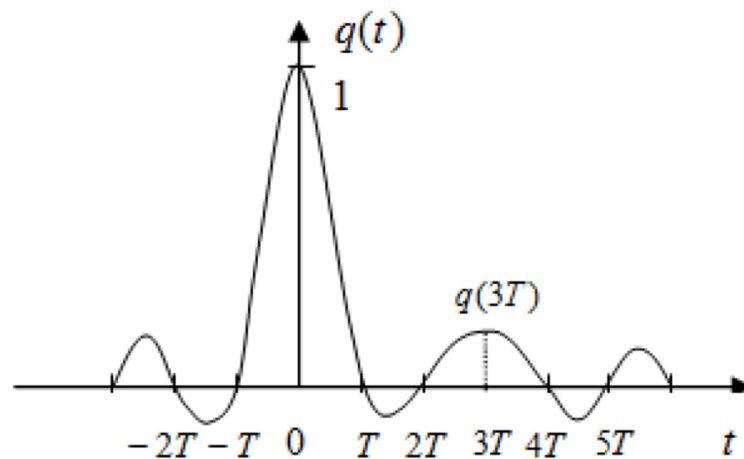


Рисунок 2.5 – Імпульсна реакція на виході фільтра

2.5. Вплив корельованих завад на пропускну здатність безперервного каналу

При дослідженні пропускну здатності каналів з флуктуаційними параметрами доцільним є використання геометричної інтерпретації випадкових величин із різним ступенем взаємної кореляції. У такому підході реалізацію коливання $U_{\text{рк}} = U_{\text{ск}} + U_{\text{шк}}$ на вході приймача можна подати у вигляді n -вимірного вектора [39], який є сумою векторів реалізації корисного сигналу $U_{\text{ск}}$ та адитивної завади $U_{\text{шк}}$ (рис. 2.6,а).

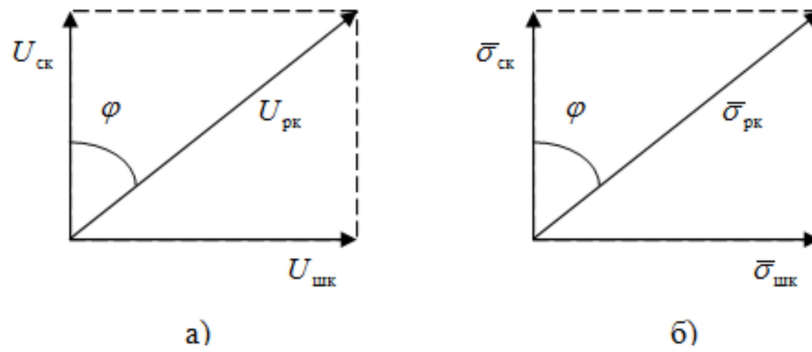


Рисунок 2.6 – Векторне представлення сигналів

У приймальному пристрої рішення щодо реєстрації сигналу приймається на основі того, який із сигналів виявляється найближчим до фактичного коливання, що надійшло. Як критерій прийому доцільно використовувати деяке порогове значення кута φ_0 між векторами $U_{ск}$ та $U_{рк}$. Якщо вектор $U_{рк}$ виходить за межі цього кута, виникає помилка. Коефіцієнт кореляції між векторами $U_{ск}$ та $U_{рк}$ визначається виразом [55]:

$$\rho_{ср} = \frac{E[U_{ск}U_{рк}]}{\sqrt{E[U_{ск}^2]E[U_{рк}^2]}},$$

де математичне очікування добутку випадкових величин описується інтегралом [55] $E[U_{ск}U_{рк}] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} U_{ск}U_{рк} \omega(U_{ск}U_{рк})dU_{ск}dU_{рк}$. Математичне очікування квадратів складових мають наступний вигляд $E[U_{ск}^2] = \sigma_{ск}^2$; $E[U_{рк}^2] = \sigma_{рк}^2 = \sigma_{ск}^2 + \sigma_{шк}^2$. Оскільки вектори $U_{ск}$ та $U_{шк}$ є незалежними, то:

$$\rho_{ср} = \frac{\sigma_{ск}}{\sigma_{рк}} = \frac{\sigma_{ск}}{\sqrt{\sigma_{ск}^2 + \sigma_{шк}^2}}. \quad (2.34)$$

Таким чином, векторна діаграма випадкових векторів $U_{ск}$, $U_{шк}$ та $U_{рк}$ (рис. 2.6, а) може бути подана у вигляді еквівалентної діаграми не випадкових векторів $\sigma_{ск}$, $\sigma_{шк}$ та $\sigma_{рк}$ (рис. 2.6, б). У цьому випадку коефіцієнт кореляції

Синфазна складова $\tilde{a}_1$, яка повністю корельована з сигналом, формує сумарний сигнал [38]:

$$U_{co} = \bar{\sigma}_c + \rho_{cш} \bar{\sigma}_{ш}. \quad (2.37)$$

Ортогональна складова $\tilde{a}_2$ некорельована з сигналом та створює сумарну заваду [38]:

$$U_{шo} = \sqrt{\bar{\sigma}_{ш}^2 + (1 - \rho_{cш}^2) \bar{\sigma}_{ш}}. \quad (2.38)$$

У результаті загальне коливання визначається як:

$$U_p = \sqrt{U_{co}^2 + U_{шo}^2}. \quad (2.39)$$

Коефіцієнт кореляції між U_{co} та $U_{шo}$ дорівнює:

$$\rho_{cp} = \cos \phi_2 = \sqrt{\frac{U_{co}^2}{U_{co}^2 + U_{шo}^2}}. \quad (2.40)$$

Підставивши вираз (2.39) у (2.40), отримуємо співвідношення для пропускної здатності однопроменевого каналу з корельованими шумами:

$$C = \Delta f_k \log_2 \left(\gamma + \frac{P_c}{P_n + P_{ш}} \right); \quad (2.41)$$

де параметр

$$\gamma = \frac{\left(1 + \rho_{cш} \sqrt{\frac{P_{ш}}{P_c}} \right)^2}{1 - \rho_{cш} \frac{P_n}{P_{ш} + P_{ш}}} \quad (2.42)$$

визначається рівнем кореляції між сигналом і шумами.

Кореляційні властивості сигналу та шуму зручно ілюструвати за допомогою векторної діаграми (рис. 2.7, б), де:

- $\bar{\sigma}_c$ і $\bar{\sigma}_{ш}$ – вектори, що відповідають середнім квадратичним значенням сигналу та корельованих шумів;
- $\rho_{сш} = \cos^2 \varphi$ – коефіцієнт кореляції між сигналом і шумом;
- $\bar{\alpha}_1, \bar{\alpha}_2$ – синфазна та ортогональна складові шумів;
- U_{co} – сумарний сигнал;
- U_p – результуюче коливання на вході приймача.

Коефіцієнт кореляції між U_{co} та U_p , який кількісно описується величиною $\cos^2 \varphi$, визначається виразом:

$$\rho_{cp} = \frac{1}{\sqrt{1 + \frac{(1 - \rho_{сш}^2) P_{шк}}{\sqrt{P_c} + \rho_{сш} \sqrt{P_{шк}}}}} \quad (2.43)$$

Таким чином, пропускна здатність каналу набуває вигляду [39]:

$$C = \Delta f_k \log_2(1 + \gamma h_{сш}^2), \quad (2.44)$$

де:

$$\gamma = \frac{\left(1 + \frac{\rho_{сш}}{\sqrt{h_{сш}^2}}\right)^2}{1 - \rho_{сш}^2} \quad (2.45)$$

та

$$h_{сш}^2 = \frac{P_c}{P_{шк}}, \quad (2.46)$$

враховують вплив корельованих шумів.

Вираз (2.45) подано графічно на рис. 2.8. Із нього видно, що пропускна здатність C суттєво залежить як від коефіцієнта кореляції $\rho_{сш}$, так і від відношення сигнал/шум $h_{сш}^2$.

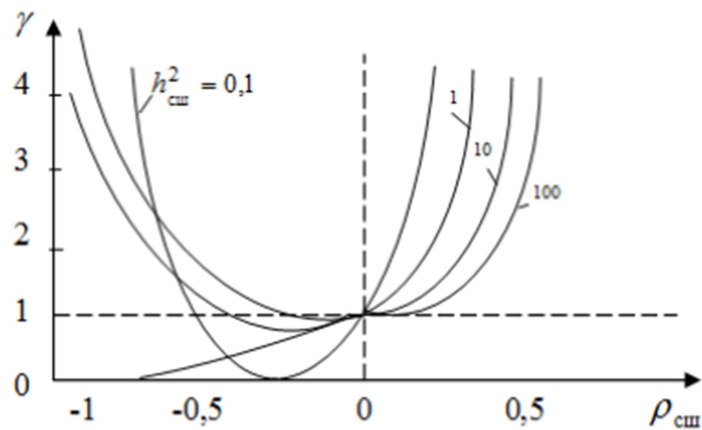


Рисунок 2.8 – Залежності $\gamma(\rho_{\text{сш}}, h_{\text{сш}}^2)$

Якщо $\rho_{\text{сш}} > 0$, то спостерігається зростання C , що зумовлено наявністю синфазної складової шуму, жорстко корельованої із сигналом. У випадку $\rho_{\text{сш}} < 0$ з'являється протифазна складова шумів, яка також має сильну кореляцію з сигналом. За певного значення $h_{\text{сш}}^2$ ця складова спочатку урівноважує сигнал, що призводить до зменшення пропускної здатності до нуля. Однак зі збільшенням її впливу вона починає перевищувати сигнал і фактично бере на себе роль носія інформації, унаслідок чого C знову починає зростати.

2.6. Компенсація надлишковості в блокових завадостійких кодах за допомогою таймерних сигналів

Однією з ключових проблем сучасних інформаційно-комунікаційних систем є забезпечення надійності передавання даних у завадових умовах [50, 51]. Для досягнення високої достовірності традиційно використовується введення надлишковості у сигнально-кодові конструкції. Водночас надмірна надлишковість призводить до зниження ефективності використання смуги пропускання каналу та збільшення часу передавання. Тому актуальним є завдання компенсації надлишковості, що передбачає оптимальне співвідношення між рівнем захищеності та швидкістю передачі. Основною метою дослідження є розробка підходу до компенсації надлишковості в

блокових коректуючих кодах шляхом використання таймерних сигналів [48-50] у бінарних каналах, що описуються моделлю Гільберта.

Для опису реальних каналів розглянемо можливості застосування моделі Гільберта. Вона є двостановою марковською моделлю потоку помилок у каналі, де зміна станів відбувається за однорідним ланцюгом Маркова [50, 51]. У «хорошому» стані перевищення сигналу h_c^2 над пороговим рівнем $h_{c_n}^2$ є значним, що зумовлює істотно нижчу ймовірність спотворення символів порівняно із середнім значенням $p_{e2} \gg p_e$. У «поганому» стані, навпаки, величина сигналу є меншою за порогову $h_c^2 < h_{c_n}^2$, що призводить до суттєвого зростання ймовірності помилок $p_{e2} \gg p_e$. Моменти переходів між станами відповідають появі пакетів помилок довжиною l_n символів. При цьому передбачається, що як окремі помилки всередині пакета, так і самі пакети є статистично некорельованими.

Ймовірність виникнення помилки на приймальному боці залежить від величини перевищення сигналу над рівнем шумів h_c^2 . Припускається, що в каналі діють адитивні гауссівські шуми, а завмирання зумовлюють випадкові зміни h_c^2 . Для отримання залежності ймовірності помилки $p_e(h_c^2)$ необхідно перейти від щільності розподілу випадкової величини $w(U_c)$ до щільності розподілу $w(h_c^2)$. Відповідно до теореми про перетворення розподілів імовірностей [56]:

$$w(h_c^2) = w[f(h_c^2)] \frac{df(h_c^2)}{dh_c^2}, \quad (2.47)$$

де функція перетворення має вигляд:

$$f(h_c^2) = U_c^2 = 2h_c^2\sigma_{\text{ш}}^2, \quad (2.48)$$

де $\sigma_{\text{ш}}^2$ – дисперсія гауссівського шуму.

З урахуванням завмирань та появи пакетів помилок розглянута модель каналу характеризується такими параметрами: p_{π} – ймовірність появи пакета помилок, яка одночасно є ймовірністю переходу каналу з "хорошого" стану в "поганий"; $p(l_{\pi})$ – ймовірність утворення пакета помилок довжиною l_{π} у поганому стані каналу; p_{e1} – ймовірність спотворення символів у хорошому стані каналу (за відсутності пакета помилок); p_{e2} – ймовірність спотворення символів у поганому стані (всередині пакета помилок).

Розглянемо ймовірність появи пакетів помилок у каналах моделі Гільберта. Припустимо, що у пакетах зосереджено $\alpha_0\%$ усіх помилок, тоді виконується співвідношення [51, 55]:

$$\int_0^{h_{c\pi}^2} f(h_c^2) w(h_c^2) dh_c^2 = \alpha_0 \int_0^{\infty} f(h_c^2) w(h_c^2) dh_c^2 = \alpha_0 p_e \quad (2.49)$$

де p_e – середня ймовірність спотворення символів.

Ймовірності помилок у хорошому p_{e1} та поганому p_{e2} станах каналу визначаються як:

$$p_{e1} = \frac{\int_{h_{c\pi}^2}^{\infty} f(h_c^2) w(h_c^2) dh_c^2}{\int_{h_{c\pi}^2}^{\infty} w(h_c^2) dh_c^2}; \quad p_{e2} = \frac{\int_0^{h_{c\pi}^2} f(h_c^2) w(h_c^2) dh_c^2}{\int_0^{h_{c\pi}^2} w(h_c^2) dh_c^2}. \quad (2.50)$$

Тоді при фіксованому значенні $h_{c\pi}^2$ маємо:

$$p_{e1} = \frac{1-\alpha_0}{1-\phi_1} p_e; \quad p_{e2} = \frac{\alpha_0 p_e}{\phi_1}, \quad (2.51)$$

де

$$\phi_1 = \int_0^{h_{c\pi}^2} w(h_c^2) dh_c^2 \quad (2.52)$$

– інтегральна функція розподілу.

Середнє число викидів обвідної випадкового процесу h_c^2 вище рівня $h_{c\pi}^2$ за 1 с дорівнює [55]:

$$\nu_0 = \frac{0,85}{\sqrt{h_{co}^2 T_{30}}}, \quad (2.53)$$

а ймовірність появи пакета помилок визначається як [40]:

$$p_{\Pi} = \nu_0 T_c e^{-\nu_0 T_c}. \quad (2.54)$$

Ймовірність утворення пакета помилок довжиною l_{Π} символів можна подати у вигляді [55]:

$$p(l_{\Pi}) = \int_{(l_{\Pi}-0,5)T_c}^{(l_{\Pi}+0,5)T_c} w(t_{\Pi}) dt_{\Pi}. \quad (2.55)$$

Припустимо, що завмирання підпорядковуються закону Релея. Тоді густина ймовірності має вигляд:

$$w(h_c^2) = \frac{2\sqrt{h_c^2}}{h_{co}^2} e^{-\frac{h_c^2}{h_{co}^2}}, \quad (2.56)$$

де h_{co}^2 – середнє значення h_c^2 .

У цьому випадку при некогерентному прийманні отримаємо [51]:

1) для "хорошого" стану каналу:

$$p_{e1} = \frac{1}{2} e^{-\frac{h_c^2}{2}}, \quad (2.57)$$

2) для "поганого" стану каналу:

$$p_{e2} = \frac{1}{2+h_{co}^2}. \quad (2.58)$$

Для значення показника $\alpha_0 = 0,99$ маємо:

$$h_{\text{сп}}^2 \approx 3; \quad \phi_1 = 1 - e^{\frac{9}{h_{\text{co}}^2}} \approx \frac{9}{h_{\text{co}}^2}. \quad (2.59)$$

При $h_{\text{co}}^2 \geq 100$, що є типовим на практиці, ймовірності приймають вигляд:

$$p_{e1} \approx 10^{-2} p_e, \quad p_{e2} \approx 0,11 p_e h_{\text{co}}^2, \quad (2.60)$$

а розподіл довжини пакетів помилок визначається як [55]:

$$p(l_{\text{п}}) = \exp\left[-\frac{\pi(l_{\text{п}}-0,5)^2}{4l_{\text{по}}^2}\right] - \exp\left[-\frac{\pi(l_{\text{п}}+0,5)^2}{4l_{\text{по}}^2}\right], \quad (2.61)$$

де $l_{\text{п}}$ – середня довжина пакета помилок у символах.

Відомо, що в каналах моделі Гільберта завадостійкість у "хорошому" стані у сотні разів перевищує завадостійкість у "поганому" стані. Разом із тим, спроби підвищити швидкість передавання інформації за рахунок зменшення тривалості елементарної посилки (тобто використання наднайквістової швидкості) призводять до виникнення значних міжсимвольних завад. Це свідчить про відсутність симетричних можливостей перетворення швидкості передавання в якість та, навпаки, якості у швидкість. Основна причина таких обмежень полягає у фіксованій тривалості одиничного елемента сигналу, яка визначається смугою пропускання каналу:

$$t_0 = \frac{1}{\Delta F} \left(\text{або } t'_0 = \frac{1}{2\Delta F} \right). \quad (2.62)$$

Енергетична відмінність між сигнальними конструкціями при поелементному способі передавання визначається енергією одиничного елемента сигналу. Для коректуючих кодів ця відмінність зростає у k разів, де k – число додаткових елементів, що вводяться для підвищення завадостійкості. Щоб збільшити кількість переданої інформації на заданому часовому інтервалі,

доцільно застосовувати такі сигнальні конструкції, у яких відстані між моментами модуляції в межах однієї кодової конструкції не менші за найквістовий інтервал, тоді як енергетична відстань між самими кодовими конструкціями визначається елементом меншої тривалості. Цим вимогам відповідають лише таймерні сигнали [50, 51]. На відміну від розрядно-цифрового кодування, де інформація про переданий розряд визначається видом сигналу на одиничному (найквістовому) інтервалі, у ТСК інформація закладається у тривалостях кількох часових відрізків сигналу τ_c в межах інтервалу конструкції T_c та їх взаємному розташуванні. Для зменшення міжсимвольних спотворень тривалість цих відрізків береться не меншою за найквістовий інтервал: $t_c = t_0 + k\Delta$ ($k \in 0, 1, \dots, I$), де часовий відрізок Δ показує частку одиничного елемента ($t_0 > \Delta = \frac{t_0}{s}$) та визначається як параметрами завад у каналі, так і допустимою ймовірністю помилкового приймання сигнальної конструкції ($s \in 2, 4 \dots 5$).

Оцінимо ефективність використання таймерних сигнальних конструкцій під час передавання через двійковий симетричний канал. На рис. 2.4 показано приклади реалізацій ТСК. Для такого способу формування сигнальних конструкцій кількість можливих реалізацій $N_{\text{рт}}$ на інтервалі $T_c = mt_0$ при $\Delta = \frac{1}{s}$ визначається виразом [51]:

$$N_{\text{рт}} = \frac{[m \cdot s - i \cdot (s-1)]!}{i! \cdot [s \cdot (m-i)]!}, \quad \tau_c \geq \Delta(s+i), \quad i = 1; 2; \dots \quad (2.63)$$

У випадку використання конструкцій з різною кількістю ЗММ число реалізацій таймерних сигналів визначається сумою [50, 51]:

$$N_{\text{рт}} = \sum_{i=1}^m \frac{[m \cdot s - i \cdot (s-1)]!}{i! \cdot [s \cdot (m-i)]!}. \quad (2.64)$$

Для оцінки ефективності було проведено розрахунки кількості реалізацій на інтервалах із довжиною $m = 5$ та 8 при значеннях числа інформаційних

моментів модуляції $i = 3$ та 4 , а також для різних величин $\Delta = \frac{t_0}{s}(s = 5; 7)/s$, де $s=5$ та 7 . Розрахунки виконувалися згідно з формулою (2.64) для наборів параметрів m , s та i . Результати подано в табл. 2.2. Серед усіх дозволених для передавання ТСК (де окремі відрізки $\tau_{ci} \geq s\Delta$, сформовані на інтервалі $T_c = mt_0$ для вибраної, можна виділити групи: $N_p(1)$ – конструкції з одним інформаційним ЗММ; $N_p(2)$ – конструкції з двома ЗММ; ... , $N_p(m-1)$ – конструкції з $(m-1)$ ЗММ; $N_p(m)$ – конструкції, які має усі ЗММ.

Загальне число реалізацій визначається як:

$$N_{\Sigma} = N_p = N_p(1) + N_p(2) + \dots + N_p(m-1) + N_p(m). \quad (2.65)$$

Таблиця 2.2 – Число реалізацій ТСК при зміні i та Δ_c

i	$\begin{matrix} s \\ m \end{matrix}$	5	7
3	5	286	1771
	8	969	6545
4	5	126	3876
	8	495	20475

Оскільки у сумарному числі N_p різним групам відповідає різна кількість кодових комбінацій із певним числом моментів модуляції, середнє значення їх кількості визначається виразом [40]:

$$\left. \begin{aligned} \bar{i} &= \sum_{i=1}^m P[N_p(i)] \cdot i \\ P[N_p(i)] &= \frac{N_p(i)}{N_{p\Sigma}} \end{aligned} \right\}. \quad (2.66)$$

Кожна ТСК при рівноймовірних символах на вході здатна передати

$$H_i = \log_2 N_p \quad (2.67)$$

біт інформації. Водночас, оскільки на вході каналу формуються кодові сигнали, що належать різним групам за числом переходів, кількість інформації, пов'язаної з вибором групи з i -переходами, дорівнює [50, 51]:

$$H_r = - \sum_{i=1}^m P[N_p(i)] \log_2 P[N_p(i)] = \sum \frac{N_p(i)}{N_p} \log_2 \left[\frac{N_p(i)}{N_p} \right]. \quad (2.68)$$

Якщо приймач отримав сигнал з i -переходами, то невизначеність у достовірності передавання кожного з них на k -му місці визначається умовною ентропією [50, 55]:

$$H\left(\frac{Z_i}{K_i}\right) = - \sum_{i=1}^{Z_0} P\left(\frac{Z_i}{K_i}\right) \log_2 P\left(\frac{Z_i}{K_i}\right), \quad (2.69)$$

де $P\left(\frac{Z_i}{K_i}\right)$ – ймовірність отримання переходу на позиції Z_i за умови, що він був переданий на позиції K_i .

Виходячи з (2.69), кількість інформації, яка передається одним словом таймерного сигналу в каналі без завад, дорівнює [50, 55]:

$$I = H_i - H_{\Sigma i} = \log_2 N_p - \sum_{i=1}^m P(i) H\left(\frac{Z_i}{K_i}\right). \quad (2.70)$$

У випадку нерівномірних довжин кодових слів середнє значення кількості інформації, що припадає на один найквістовий елемент, визначається виразом [50, 55]:

$$I_0 = \frac{I}{\bar{m}_\Sigma} = \frac{\log_2 N_p - \sum_{i=1}^m i P(i) H\left(\frac{Z_i}{K_i}\right)}{\sum_{i=1}^m \left[i t_0 + \frac{m t_0 - i t_0}{2} \right] \frac{N_p(i)}{N_p}} \quad (2.71)$$

де $\bar{m}_\Sigma$ – середня довжина кодового слова.

Слід зазначити, що використання сигналів із нерівномірною довжиною можливе лише за умови наявності спеціальних ознак, які вказують на кінець кодового слова. Тому при формуванні простих таймерних сигнальних

конструкції доцільно застосовувати кодові сигнали однакової довжини $T_0 = mt_0$. Для такого випадку пропускна здатність виражається простішим співвідношенням [50, 55]:

$$I_0 = \frac{\log_2 N_p - \sum_{i=1}^m i P(i) H\left(\frac{Z_i}{K_i}\right)}{m}. \quad (2.72)$$

Із виразу (2.72) можна зробити висновок, що пропускна здатність каналу при використанні таймерних сигналів визначається двома основними параметрами: загальною кількістю можливих комбінацій N_p та достовірністю правильної реєстрації кожного ЗМВ в приймачі.

Оцінимо ефективність компенсації ТСК надлишковості в блокових кодах на прикладі коду Слепяна (9,5) [56] для каналу Гільберта. Для цього розглянемо блоковий код Слепяна (9,5) за наступними параметрами: довжина кодового блоку $n = 9$; кількість інформаційних біт $m = 5$, кількість перевірочних біт $r = n - k = 4$; мінімальна кодова відстань $d = 3$. На один інформаційний біт припадає $r/k = 0,8$ перевірочних елементів, що істотно знижує кодову швидкість. Мета дослідження полягає в тому, щоб показати, як за допомогою ТСК можна компенсувати цю надлишковість, зберігши або підвищивши завадостійкість у каналі, який описується моделлю Гільберта.

Для оцінки ефективності компенсації надлишковості коду при передаванні ТСК приймемо $\Delta = 0,2t_0$ ($s = 5$). Середньоквадратичне відхилення ЗММ задано як $\sigma_0 = 0,017 < 0,02$ [56]. Оскільки для виправлення двократних помилок необхідна кодова відстань $d = 5$, а кількість перевірочних елементів становить 8, для синтезу множини реалізацій ТСК можна використати всі сигнальні конструкції на інтервалі $T_c = 6,7t_0$ при $i \in \overline{1 \dots 6}$, ($N_{p\Sigma} = 9494$). Ймовірність помилкового приймання одного ЗММ у «хорошому» стані каналу визначається як:

$$P_{\text{пп}} = 2Q\left(\frac{\Delta}{2\sigma_0}\right),$$

де $Q(\cdot)$ – функція Лапласа. Для заданих параметрів отримаємо:

$$P_{\text{пп}}^1 = 2 \cdot \left[0,5 - \Phi \left(\frac{20}{2 \cdot 0,02} \right) \right] = 5,8 \cdot 10^{-7}.$$

В цьому випадку ймовірність вірного приймання одного ЗММ у сигнальній конструкції ТСК: $P_{\text{вп}}^{(1)} = 1 - P_{\text{пп}} = 0,99999942$. Оскільки використовуються сигнальні конструкції з різною кількістю ЗММ $i \in (1 \dots 6)$, середнє значення становить $\bar{i} = \frac{\sum_{i=1}^m i \cdot C_{mS-i(S-1)}^i}{\sum_{i=1}^m C_{mS-i(S-1)}^i} = 4$, тоді ймовірність вірного приймання всієї сигнальної конструкції $P_{\text{вп}} = (0,99999942)^4 = 0,9999976$.

Враховуючи, що одна сигнальна конструкція ТСК несе інформацію про 13-елементні комбінації РЦК, ймовірність вірного приймання одного елемента після перекодування ТСК у РЦК (у «хорошому» стані каналу) становитиме $P_{e \text{ вп}} = \sqrt[13]{P_{\text{вп}}} = 0,999999875$, а ймовірність помилкового приймання одного елемента: $P_e^* = 2 \cdot 10^{-7}$. Це значення є більш ніж на чотири порядки меншим за ймовірність помилкового приймання елемента при використанні розрядно-цифрового кодування: $P_{e \text{ р}} \approx (1,8 \dots 2,3) \cdot 10^{-3}$. Отже, можна стверджувати, що сумарна ймовірність помилкового приймання після перетворення ТСК у РЦК буде істотно меншою. Це пояснюється тим, що таймерні сигнальні конструкції формуються на інтервалі $T_c = 6,7t_0$ на відміну від 13-елементних кодових слів у РЦК. Відповідно, відношення тривалостей становить $k = \frac{6,7}{13} = 0,515$, що означає зменшення ймовірності перебування каналу у «поганому» стані під час передавання одного ТСК майже вдвічі порівняно з РЦК. Враховуючи, що 13-елементний код здатний виправляти помилки кратності до двох, загальна ймовірність правильного приймання комбінації визначається сумою ймовірностей подій: усі 13 елементів передано вірно або ж з них спотворено не більше двох. Відповідно: $P_{\text{пр}} = (0,999999875)^{13} + 13 \cdot (0,999999875)^{12} \cdot 0,001 + 78 \cdot (0,999999875)^{11} \cdot 10^{-6} = 0,9999996$. Для

порівняння з ймовірністю правильного приймання елементів первинного коду обчислимо еквівалентну ймовірність $P_{e\ p}$, враховуючи, що в початковому кодовому слові міститься $m=5$ інформаційних елементів $P_{e\ p} = \sqrt[5]{0,9999996} = 0,9999999$, $P_{e\ e} = 1 - P_{e\ n} = 10^{-7}$.

Проведені розрахунки підтверджують, що використання ТСК дозволяє ефективно компенсувати надлишковість 13-елементного коду з кодовою відстанню $d = 5$, побудованого на базі коду Слепяна (9,5) [51, 56]. Це забезпечує зниження ймовірності помилкового приймання більш ніж на чотири порядки та підвищення кодової швидкості майже удвічі (з 5/13 до 5/6,7). Аналіз отриманих результатів показав, що застосування ТСК у поєднанні з кодом Слепяна (9,5) забезпечує підвищення ефективності передавання інформації, зокрема:

1) ймовірність помилкового приймання елемента знижується з величини $P_{e\ p} \approx (1,8 \dots 2,3) \cdot 10^{-3}$ для розрядно-цифрового кодування до $P_e^* = 2 \cdot 10^{-7}$, тобто більш ніж на чотири порядки;

2) загальна ймовірність правильного приймання комбінації становить $P_{np} = 0,9999996$, що еквівалентно еквівалентній ймовірності вірного приймання одного елемента $P_{e\ p} = 0,9999999$;

3) кодова швидкість зростає з $R=5/13 \approx 0,38$ до $R=5/6,7 \approx 0,75$, тобто майже вдвічі.

Отже, запропонований алгоритм не лише скорочує часові витрати на передавання інформації приблизно удвічі, але й забезпечує істотне зниження ймовірності помилки, що свідчить про підвищення завадостійкості та якості приймання інформації в каналах моделі Гільберта.

2.7. Інформаційні параметри кодів Слепяна з компенсацією надлишковості таймерними сигналами

Для забезпечення прийнятної якості функціонування системи передавання інформації в нестационарному каналі зв'язку необхідно підтримувати ймовірність помилки (вірогідність правильного передавання) на рівні, що не перевищує певного гранично допустимого значення. Щоб бути інваріантною до завад у каналі, система повинна володіти здатністю оцінювати якість каналу, прогнозувати його поведінку та адаптуватися до змінних умов передавання. Для реалізації такого адаптивного механізму застосовуються різні види сигнальної надлишковості. Однією з найважливіших характеристик цифрових систем зв'язку є їхня завадостійкість, яка може бути досягнута як завдяки ефективним методам приймання й обробки сигналів, так і за рахунок використання завадостійкого кодування. Ефективність СП істотно підвищується при застосуванні сучасних методів модуляції та завадостійкого кодування, що дозволяють більш повно реалізувати пропускну здатність каналу з одночасним забезпеченням високої достовірності передавання.

У працях [51, 56] розглянуто проблеми підвищення ефективності передавання та обробки сигналів. Проте з огляду на широке впровадження обчислювальної техніки й автоматизованих систем управління у всі сфери життєдіяльності людини виникає потреба у подальшому розвитку методів передавання інформації, які б забезпечували обмін даними з високою швидкістю та заданим рівнем достовірності. Метою даного підрозділу є визначення та порівняння інформаційної ємності найквістового елемента для кодів Слепяна і таймерних сигнальних конструкцій.

Розглянемо принцип формування простих і надлишкових позиційних кодів. У техніці зв'язку застосовуються семантичні та елементні коди. До семантичних кодів належать комбінації з кількох букв, які позначають цілі фрази [51]. Наприклад, у міжнародному радіозв'язку використовуються такі поєднання: SOS – сигнал лиха, TTT – сигнал безпеки. Широке поширення

отримали також так звані Z-коди або Q-коди, у яких на початку кодових слів стоять символи Z чи Q, що вказують на певні фрази. Наприклад: ZSU – «ваші сигнали нерозбірливі»; QKM – «мені заважають на цій хвилі». Елементні коди відрізняються тим, що кожному символу (букві) ставиться у відповідність певне число у заданій системі числення [4]. Наприклад, у табл. 2.3 і табл. 2.4 подано записи десяткових чисел у різних варіантах чотирьохелементних двійкових кодів, які відображають послідовність чисел на певному відрізку числової осі. Серед складених кодів найбільше поширення отримали двійкові-десяткові коди. Такі коди зазвичай використовуються як проміжні під час перетворення десяткових чисел у двійкову систему та навпаки. Наприклад, це актуально при введенні у обчислювальну машину даних, поданих у десятковій системі, або при виведенні з неї інформації для подальшої реєстрації в десятковій формі [50, 51].

Таблиця 2.3 – Подання чисел у різних системах числення

Число					
Десяткове число	Десяткове число	Десяткове число	Десяткове число	Десяткове число	Десяткове число
0	0	0000	8	8	1000
1	1	0001	9	9	1001
2	2	0010	10	A	1010
3	3	0011	11	B	1011
4	4	0100	12	C	1100
5	5	0101	13	D	1101
6	6	0110	14	E	1110
7	7	0111	15	F	1111

У двійковому-десятковому коді основною системою числення є десяткова. Однак кожна цифра десяткового числа подається у вигляді чотирирозрядного двійкового числа (тетради). Для фіксації цифр десяткового числа найбільше практичне застосування знайшли чотириелементні двійкові вагові коди: 8–4–2–1; 7–4–2–1; 5–1–2–1 та 2–4–2–1. Цифри у назві коду визначають вагу (кількість

одиниць) у відповідних двійкових розрядах (табл. 2.4). Кількість двійкових цифр K при двійковому поданні визначається максимальним номером переданих повідомлень у десятковій системі (N_{10}) [4]:

$$K = E^+[\log_2 N_{10}], \quad (2.73)$$

де: E^+ позначає округлення до найближчого більшого цілого числа.

Для забезпечення можливості виявлення або виправлення помилок до k елементів простого коду (2.73) додають r перевірочних елементів. Перевірочні елементи надлишкового коду формуються у вигляді сум певних інформаційних елементів простого коду.

Таблиця 2.4 – Подання десяткових чисел у різних чотириелементних двійкових кодах

Десятичное число	Код 8-4-2-1	Код 7-4-2-1	Код 5-1-2-1	Код 2-4-2-1
0	0000	0000	0000	0000
1	0001	0001	0001	0001
2	0010	0010	0010	0010
3	0011	0011	0011	0011
4	0100	0100	0111	0100
5	0101	0101	1000	1011
6	0110	0110	1001	1100
7	0111	1000	1010	1101
8	1000	1001	1011	1110
9	1001	1010	1111	1111

У табл. 2.5 наведені значення номерів інформаційних елементів кодів Слепяна, які беруть участь у формуванні відповідних перевірочних елементів r

для $n \in 5 \dots 16$. З таблиці бачимо, що кількість сум відповідає різниці $(n - k)$, а всі контрольні суми повинні дорівнювати нулю. У стовпцях N_1, N_2, N_3, N_4 табл. 2.5 у чисельнику вказана кількість можливих помилок, а у знаменнику – число помилок, які можуть бути виправлені при відповідній кратності, а також кодова відстань d для відповідного коду. Оцінимо кількість можливих помилок $N_i(n)$ кратності $tt_{\text{пом}} \in 1 \dots n$ згідно з виразом [33]:

$$N_i(n) = C_n^i = \frac{n!}{i! \cdot (n-i)!}, \quad (2.74)$$

де: $i \in 1 \dots n$. Результати обчислень питомої ваги виявлених та виправлених помилок кодами Слепяна для кратності помилок $t_{\text{ош}} \in 1 \dots 4$ наведено у стовпцях N_1, N_2, N_3, N_4 . Дані подано у вигляді дробів: у чисельнику зазначено максимальне число виправлених помилок, а у знаменнику – загальне число можливих помилок відповідної кратності (2.74). З табл. 2.5 бачимо, що зі збільшенням кількості перевірочних елементів зростає частка помилок, що виправляються, однак одночасно зменшується ефективність використання коду. Ефективність визначається співвідношенням:

$$\eta = \frac{P(\geq 1, n)}{P(\geq 1, n) - P_{\text{исп}}(n)}, \quad (2.75)$$

де $P_{\text{исп}}(n)$ – ймовірність виправлення помилок відповідної кратності. Оцінимо інформаційні параметри кодів Слепяна. Кількість інформації (ентропія H) кодового слова визначається лише числом інформаційних елементів у слові k [1] та кількістю можливих значень інформаційного параметра a [39]:

$$N_p = a^k; H = \log N_p = \log_2 a^k = k \log_2 a. \quad (2.76)$$

Оскільки у кожному кодовому слові довжиною n інформація міститься лише в k елементах, то обсяг інформації у двійкових кодових словах різних кодів Слепяна (ентропія H) дорівнює k біт. У табл. 2.6 наведено значення

обсягу інформації (H) у бітах у кожному кодовому слові та інформаційну ємність одного найквістового елемента згідно з виразом J_n [32]:

$$J_n = k/n, \quad (2.77)$$

де: k – число інформаційних елементів; n – загальна кількість елементів. З табл. 2.6 бачимо, що ентропія кодового слова визначається виключно кількістю інформаційних елементів. У простих, так і у надлишкових кодах, ентропія завжди визначається k інформаційними елементами. Оскільки в надлишкових кодах загальна кількість елементів дорівнює:

$$n = k + r, \quad (2.78)$$

де k – кількість інформаційних біт, r – кількість перевірочних біт.

Таблиця 2.6 – Значення обсягу інформації H та ємності одного найквістового елемента J_n для кодів Слепяна

n, k	5,2	6,3	7,4	8,4	9,5	10,5	10,6	11,5	11,6	12,7
H	2	3	4	4	5	5	6	5	6	7
J_n	0,4	0,5	0,57	0,5	0,55	0,5	0,6	0,45	0,54	0,63

В цьому випадку інформаційна ємність одного елемента кодів Слепяна задовольняє умові $J_n < 1$. У табл. 2.6 наведено розрахунки лише для двійкового каналу ($a = 2 \rightarrow 0; 1$). З виразів (2.76) та (2.77) випливає, що інформаційна ємність найквістового елемента визначається числом можливих значень інформаційного параметра a . Якби число значень параметра a було збільшено до 4, кожен елемент коду містив би $\log_2 4 = 2$ біти інформації. У структурі кодових слів, сформованих за алгоритмом табл. 2.5, інформаційна ємність найквістового елемента I_n для двійкового каналу здебільшого дорівнює 0,5 (табл. 2.6), що свідчить про низьку ефективність використання часу передачі кодової конструкції Слепяна.

Таблиця 2.5 – Номера інформаційних елементів кодів Слеп'яна для формування перевірочних символів

n, k код	Номера перевірочних елементів								Кратність помилок, що виправляються				
	1	2	3	4	5	6	7	8	N_1	N_2	N_3	N_4	d
5,2	12	2	1						5/5	2/10			3
6,3	12	12	23						6/6	1/15			3
7,4	134	124	123						7/7				3
8,4	134	124	123	1234					8/8	7/28			3
9,5	1345	1245	1235	1234					9/9	6/36			3
10,5	1345	1245	1235	1234	12345				10/10	21/45			3
10,6	1345	1245	12356	12346					10/10	5/45			3
11,5	123	124	134	234	125	135			11/11	46/55	6/165		4
11,6	13456	12456	12356	12346	12345				11/11	20/55			4
11,7	1345	12457	12356	123467					11/11	4/55			3
12,5	123	124	234	1235	45	1245	1345		12/12	63/66	52/220		5
12,6	12456	2356	1346	1345	124	123			12/12	50/66	1/220		4
12,7	13456	12456	123567	123467	123457				12/12	19/66			4
12,8	1235678	12346	12457	13458					12/12	3/66			3
13,5	123	124	134	125	135	245	345	12345	13/13	78/78	152/286	12/715	5
13,6	13456	1256	1246	1236	1245	1235	1234		13/13	72/78	42/286		4
13,7	23567	3467	2457	2456	1235	1234			13/13	50/78			4
14,6	1235	1246	1346	156	2346	256	356	456	14/14	91/91	150/364	14/1001	5
14,8	34678	4578	13568	3567	12346	12345			14/14	49/91		14/1001	4
15,9	2345	1234	245	4789	15789	1459			15/15	48/105		15/1365	4
16,10	1245	4579	24689	124510	134610	35610			16/16	47/120		16/1820	4

Як зазначено у [51], збільшити інформаційну ємність при позиційному кодуванні можливо лише шляхом збільшення числа значень інформаційного параметра a , що неможливо для двійкового каналу. Підвищити ефективність використання часу реалізації сигнальних конструкцій у двійкових каналах можна лише за рахунок застосування таймерного кодування [50, 51].

2.8. Підвищення ефективності використання інтервалу реалізації коду Сліпяна

З виразу (2.76) випливає, що для збільшення ентропії на заданому інтервалі часу необхідно збільшити кількість реалізацій N_p , що дозволить підвищити інформаційну ємність одного найквістового елемента у двійковому каналі, тобто забезпечити умову $J_H > 1$. Як метод підвищення ефективності використання часових інтервалів кодових конструкцій Сліпяна обрано таймерне кодування [56]. При таймерному кодуванні часові інтервали кодових конструкцій [51] кратні величині $\Delta < t_0$, при цьому інтервали між суміжними моментами модуляції не кратні найквістовому елементу, але й не менші за нього, що дозволяє реалізувати енергетичне відстань між кодовими словами, рівне енергії елемента Δ . Вибір таких сигналів забезпечує отримання на заданому інтервалі часу більшої кількості конструкцій N_p , ніж при використанні позиційного кодування ($N_p \gg 2^m$, де m – число одиничних елементів у сигнальній конструкції на інтервалі часу $T_c = mt_0$). Відомо, що [51] кількість реалізацій із заданою кількістю інформаційних відрізків визначається формулою:

$$N_{PT} = \frac{[mS - i(S-1)]!}{i!(mS-i)!}. \quad (2.79)$$

У табл. 2.7 у чисельнику наведено кількість реалізацій таймерних сигналів N_p , розраховану за виразом (2.79) для $m \in (4 \dots 10)t_0$ при $S = 7$, а в

знаменнику подано інформаційну ємність найквістового елемента, визначену виразом [56]:

$$J_H = \frac{\log_2 N_p}{m}. \quad (2.80)$$

Оцінимо ефективність використання інтервалу реалізації кодової конструкції коду Слепяна (9.5) при реалізації множини таймерних сигнальних конструкцій. Враховуючи, що код має 5 інформаційних елементів, для цього необхідно $2^5=32$ кодові конструкції. Нехай для оцінки якості передачі використовується 32 дозволених кодових слова за рівнянням якості [51]:

$$x_1 + 3x_2 + 5x_3 = 0 \bmod 7. \quad (2.81)$$

В цьому випадку необхідна множина використовуваних кодових конструкцій дорівнюватиме $32 \times 7 = 224$ кодових слова. Згідно з виразом (2.79), для отриманих 224 кодових слів при $S = 7$, $i = 3$ знадобиться час побудова сигнальних конструкцій $T_{СК} = 4t_0 + 5\Delta = 4,71t_0 \approx 5t_0$.

Таблиця 2.7 – Кількість реалізацій і інформаційна ємність при ТСК

i	M						
	4	5	6	7	8	9	10
1	22/1,11	29/0,97	36/0,86	43/0,78	50/0,71	57/0,65	64/0,6
2	120/1,73	253/1,6	435/1,46	666/1,34	946/1,24	1875/1,21	1653/1,07
3	120/1,73	680/1,88	2024/1,83	4495/1,73	8436/1,63	14190/1,53	22100/1,44
4	1/0	330/1,67	3060/1,93	12650/1,95	35960/1,89	82251/1,81	613185/1,92
5	0/–	1/0	792/1,61	11628/1,93	65780/2,00	237736/1,98	658008/1,93

Отже, замість 9-елементних кодових комбінацій позиційного коду Слепяна можна передати захищені кодові комбінації на інтервалі $T_{СК} = 5t_0$, тобто в одному найквістовому елементі ($J_H = 5/5 = 1$ біт) міститься 1 біт інформації, що майже вдвічі більше значень J_H , наведеної в табл. 2.6.

Висновки

У другому розділі проведено дослідження теоретичних і практичних аспектів підвищення завадостійкості передавання інформації в умовах РЕБ на основі сумісного використання блокових завадостійких кодів і таймерних сигналів. Отримані результати дозволили сформулювати такі висновки:

1. Показано, що адекватне моделювання дискретних каналів у складних умовах РЕБ можливе лише на основі врахування нестационарності завад, кореляційної структури сигналів та ймовірнісної природи їх спотворень. За результатами огляду математичних моделей дискретного каналу встановлено, що найбільш придатними для аналізу ефективності методів захисту інформації в таких умовах є моделі Гільберта та Маркова. Це дозволяє точніше оцінити реальні можливості каналів зв'язку щодо забезпечення необхідної достовірності передавання.

2. Досліджено вплив надлишковості на ефективність завадостійкого обміну. Встановлено, що використання додаткової кількості перевірочних символів у блокових кодах хоч і підвищує ймовірність виправлення помилок, але суттєво знижує кодову швидкість. Це потребує пошуку методів, здатних компенсувати надлишковість без втрати достовірності.

3. Обґрунтовано, що адаптивне перетворення запасу якості (ймовірності вірного приймання) у швидкість передавання інформації можливе завдяки використанню сигнальних конструкцій із змінною тривалістю елементів, прикладом яких є таймерні сигнали. Використання ТСК дозволяє виконувати обмін між показниками пропускної здатності та завадостійкості з урахуванням рівня шуму в каналі.

4. Встановлено, що міжсимвольні завади мають кореляційну залежність із корисним сигналом, що значно ускладнює їхнє усунення традиційними методами. Показано, що врахування статистичних характеристик корельованих завад є критичним для більш точного оцінювання пропускної здатності та вибору оптимальних методів кодування.

5. Виявлено, що за наявності корельованих завад пропускна здатність каналу знижується більш істотно, ніж при впливі некорельованих завад. Це підтверджує необхідність застосування спеціалізованих сигнально-кодових конструкцій, здатних зменшити негативний вплив корельованих помилок.

6. Доведено, що використання таймерних сигналів дозволяє компенсувати надлишковість блокових кодів, зменшити ймовірність помилкового приймання на кілька порядків та підвищити кодову швидкість майже вдвічі.

7. Запропоновано метод оцінювання інформаційних параметрів кодів Слепяна з урахуванням компенсації надлишковості таймерними сигналами. Показано, що поєднання часових структурних властивостей сигналів та блокового кодування забезпечує підвищення ефективності використання найквістового інтервалу.

8. Розроблено підхід до підвищення ефективності використання інтервалу реалізації кодів Слепяна, що дозволяє знизити часові витрати на передавання даних та одночасно забезпечити високий рівень достовірності.

Отримані результати свідчать, що сумісне використання блокових завадостійких кодів і таймерних сигналів є перспективним напрямом підвищення ефективності та надійності передавання даних у військових інформаційно-комунікаційних системах. Розроблені підходи створюють теоретичне підґрунтя для формування адаптивних методів захисту інформації в умовах дії потужних завад.

3 ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ НЕПОЗИЦІЙНИХ ТАЙМЕРНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ

У розділі досліджено можливості підвищення захисту інформації на основі показників завадостійкості та структурної прихованості непозиційних сигнально-кодових конструкцій, що формуються шляхом таймерного кодування. Обґрунтовано доцільність застосування таймерних сигналів у поєднанні з позиційним завадостійким кодуванням і стохастичним шифруванням для компенсації надлишковості перевірочних та випадкових елементів. Визначено залежність між кількістю можливих реалізацій сигнальних конструкцій та показником структурної прихованості. Показано, що таймерні сигнали здатні забезпечити вищу прихованість у порівнянні з класичними позиційними кодами на обмежених інтервалах часу. Водночас виявлено зворотний зв'язок між завадостійкістю та прихованістю, що зумовлює необхідність балансування параметрів кодування. Запропоновано підхід до формування множин таймерних сигнальних конструкцій, що забезпечує підвищення загального рівня захисту інформації в каналі зв'язку.

3.1. Захисту інформації від несанкціонованого доступу на основі структурної прихованості сигнальних конструкцій

Захист інформації від НСД у сучасних ІКС може бути реалізований не лише за допомогою традиційних криптографічних методів, але й через структурну прихованість сигнальних конструкцій [1-3]. Основна ідея цього підходу полягає у підвищенні складності розпізнавання складності сигналу для стороннього спостерігача шляхом використання множини альтернативних конструкцій для передачі одного й того ж інформаційного символу.

При використанні структурної прихованості інформаційний сигнал $s(t)$ модулюється таким чином, щоб його структурні параметри (наприклад, часові

інтервали між імпульсами, тривалість або положення імпульсів) формували множину можливих сигнальних конструкцій N_p . Це дозволяє забезпечити додатковий рівень прихованості на фізичному та каналному рівнях моделі OSI без застосування складних криптографічних операцій.

Математично потенційна структурна прихованість визначається як:

$$S_{\text{стр}} = \log N_p \quad (3.1)$$

де: $S_{\text{стр}}$ – фактично означає кількість біт, що характеризує ступінь структурної прихованості, а N_p – кількість можливих сигнальних конструкцій для передачі одного інформаційного символу.

Якщо один символ передається послідовністю з L імпульсів, а кожен імпульс може займати M часових позицій, то число конструкцій розраховується за формулою [50, 51]:

$$N_p = M^L, \quad S_{\text{стр}} = L \cdot \log N_p \quad (3.2)$$

Ця залежність показує, що потенційна структурна прихованість зростає при збільшенні числа імпульсів L або кількості можливих позицій M . Таким чином, навіть при передачі одного символу інформації можна досягти значного ускладнення його детектування для стороннього спостерігача. Важливим питанням є встановлення зв'язку між показниками структурною прихованістю та криптографічною стійкістю, за допомогою яких оцінюється захист інформації на різних рівнях моделі OSI. При шифруванні інформації реалізується процес перетворення відкритого повідомлення у зашифрований вигляд (шифртекст) за допомогою певного алгоритму і ключа, з метою забезпечення конфіденційності та захисту від несанкціонованого доступу. Шифрування забезпечує конфіденційність, цілісність, автентичність та

незаперечність, тобто відправник не може відмовитися від факту відправлення. Математично процес шифрування описується як функція:

$$S_{\text{шифр}} = E_K(M), \quad (3.3)$$

де M – відкрите повідомлення, E – алгоритм шифрування, K – криптографічний ключ, $S_{\text{шифр}}$ – шифртекст.

Розшифрування – це зворотний процес, який виконується за допомогою ключа та відповідного алгоритму:

$$M = D_K(S_{\text{шифр}}), \quad (3.4)$$

де D – алгоритм розшифрування.

Структурна прихованість характеризує захист інформації на фізичному та каналному рівнях (рівні 1–2 моделі OSI) [4]. Криптографічна стійкість оцінює захист інформації на мережевому, транспортному та прикладному рівнях (рівні 3–7 OSI) [40–42]. Цей вид захисту спрямований на забезпечення математичної неможливості відновлення повідомлення або ключа без знання додаткових секретних даних. Як правило, криптографічна стійкість оцінюється довжиною ключа K , тобто

$$N_K = 2^K, \quad (3.5)$$

де N_K – простір ключів криптосистеми, K – довжина ключа у бітах.

Аналогічно криптографічну стійкість можна виразити через показник інформаційної прихованості [1, 2]:

$$S_{\text{інф}} = \log 2^K = \log N_K. \quad (3.6)$$

Таким чином, і структурна прихованість, і криптографічна стійкість вимірюються у бітах та можуть бути інтерпретовані як показники ентропії. Це дозволяє інтегрувати їх у єдину модель комплексної безпеки:

$$S_{\text{інт}} = S_{\text{стр}} + S_{\text{інф}} \quad (3.7)$$

де $S_{\text{інт}}$ – інтегральна міра захисту інформації від НСД, що враховує одночасно складність виявлення сигналу у каналі та стійкість його криптографічного захисту. Порівняння показників структурної прихованості та криптографічної стійкості представлено в табл. 3.1.

Таблиця 3.1 – Порівняння структурної прихованості та криптографічної стійкості

Характеристика	Структурна прихованість	Криптографічна стійкість
Рівень дії	Фізичний та канальний рівні (1–2 рівні OSI)	Мережевий, транспортний, прикладний рівні (3–7 OSI)
Принцип дії	Використання множини сигнальних конструкцій (позиційних, таймерних, СКК системи модуляції та розширення спектра початкового сигналу тощо) для передачі одного символу	Використання криптографічного ключа для перетворення інформації
Одиниці вимірювання	Біти ентропії	Біти ентропії
Захист від НСД	Ускладнює виявлення та ідентифікацію сигналу у каналі	Ускладнює розшифрування перехопленого сигналу
Слабке місце	Після виявлення сигнал може бути прочитаний без криптографії	Сигнал легко виявити у каналі
Найвища ефективність	У поєднанні з криптографічними методами	У поєднанні зі структурною прихованістю

Можна визначити наступні варіанти реалізації структурної прихованості для інформації від НСД [2, 58, 59]:

1) використання ТСК, в яких інформація закладена в ЗММ імпульсів, що ускладнює виявлення структури сигналу без знання параметрів таймерного кодування;

2) множинність сигнальних конструкцій, коли для одного символу існує багато варіантів його передачі, що підвищує непередбачуваність сигналу;

3) незалежність від криптографічного ключа, коли структурна прихованість забезпечується навіть без використання шифрування, але може поєднуватися з криптографічними методами для підвищення стійкості системи;

4) захист на фізичному рівні, коли сигнал із високою структурною прихованістю важче виявити і ідентифікувати у шумі, що зменшує ризик НСД.

Отже, застосування структурної прихованості сигнальних конструкцій дозволяє формувати надлишкові часові та позиційні варіанти передачі, що ускладнює аналіз і детектування сигналу сторонніми особами. Цей підхід є ефективним засобом захисту інформації від НСД на фізичному та каналному рівнях, особливо у системах, де необхідно забезпечити високий ступінь невидимості переданих даних.

3.2. Аналіз позиційного та непозиційного кодування для забезпечення структурної прихованості сигнально-кодових конструкцій

Забезпечення структурної прихованості сигнально-кодових конструкцій можливе за рахунок застосування різних методів кодування, серед яких найбільш поширеними є позиційне та непозиційне кодування. Позиційне кодування базується на використанні інформації про розташування елементів у часовому або частотному просторі [50, 51]. У цьому випадку інформаційні символи кодуються шляхом вибору певної позиції сигналу серед множини можливих. Структура позиційного двійкового цифрового сигналу є відносно простою, що обмежує можливості формування додаткових реалізацій сигнально-кодових конструкцій. У такому випадку процес забезпечення структурної прихованості фактично відсутній, оскільки набір можливих станів визначається лише двома рівнями (0 та 1) з фіксованими часовими позиціями. Для двійкових позиційних сигналів забезпечення захисту інформації може здійснюватися виключно за рахунок шифрування даних. Це означає, що стійкість системи в даному випадку визначається бієктивністю криптографічного перетворення та довжиною ключа, тоді як структурна прихованість не робить суттєвого внеску в загальну безпеку захисту інформації від НСД.

Розглянемо можливість використання багаторівневого цифрового сигналу для підвищення структурної прихованості. Багаторівневі цифрові сигнали розширюють простір допустимих кодових комбінацій порівняно з двійковим представленням, що може суттєво підвищити структурну прихованості сигнально-кодових конструкцій [2, 58, 59]. Повна кількість можливих кодових слів довжини L у M -арному алфавіті без обмежень на мінімальну відстань становить:

$$N_{\text{заг бтр}} = M^L. \quad (3.8)$$

Розглянемо інформаційний вміст багаторівневого сигналу, який характеризує еквівалент у бітах:

$$I = \log_2 N_{\text{заг бтр}} = L \log_2 M. \quad (3.9)$$

Можна відзначити, що підвищення числа рівнів M лінійно збільшує кількість біт інформації, що міститься у слові довжини L , і, відповідно, експоненційно (M^L) розширює простір комбінацій. Це означає перспективність використання багаторівневих сигналів для підвищення структурної прихованості. Розглянемо кількість допустимих кодових слів за умови мінімальної відстані d_0 . Якщо накладається вимога, щоб будь-які два кодові слова мали відстань щонайменше d_0 , то максимальна кількість кодових слів позначається $A_q(L, d_0)$, де $q = M$. Точне значення $A_q(L, d_0)$ залежить від конструкції коду; проте для оцінки використовують відомі межі. Обсяг q -арної сфери Хеммінга радіуса $t = (d_0 - 1)/2$ у просторі довжини L визначається як:

$$V_q(L, t) = \sum_{i=0}^t \binom{L}{i} (q - 1)^i. \quad (3.10)$$

Ця величина рахує кількість слів, що лежать на відстані не більш ніж t від заданого слова, тобто центр сфери. Межа пакування сфер (верхня оцінка) виходить із умови, що сфери Хеммінга радіуса $t = (d_0 - 1)/2$ [39], побудовані навколо різних кодових слів, не повинні перетинатися. У такому разі::

$$A_q(L, d_0) \leq \frac{q^L}{V_q(L, t)}. \quad (3.11)$$

Ця оцінка відображає граничну кількість кодових слів, які можна розмістити у просторі q^L таким чином, щоб кулі (сфери) радіусом t навколо кожного кодового слова не перекривалися. Інакше кажучи, вона показує максимально можливе число комбінацій при заданій мінімальній відстані, а отже – верхню межу для рівня структурної прихованості. Оцінка Варшамова-Гілберта (нижня межа) гарантує, що існують коди, які досягають щонайменше такої кількості кодових слів та оцінюється за формулою:

$$A_q(L, d_0) \geq \frac{q^L}{V_q(L, d_0 - 1)}. \quad (3.12)$$

Ця оцінка визначає мінімально забезпечуваний рівень структурної прихованості для заданих параметрів L , q , d_0 . Це означає, що навіть у найгіршому випадку можна побудувати код з такою кількістю допустимих комбінацій. Межа Сінглтона впливає з простого співвідношення між довжиною коду, розмірністю та мінімальною відстанню. Для будь-якого q -арного коду справедливо:

$$A_q(L, d_0) \leq q^{L-d_0+1}. \quad (3.13)$$

За цими межами впливає, що вимога збільшення значення d_0 істотно зменшує максимально можливу кількість кодових слів $A_q(L, d_0)$ і, відповідно, знижує структурну прихованість. Отже, межі (4-6) задають діапазон можливих

значень максимальної кількості кодових слів і дозволяють оцінити компроміс між завадостійкістю та структурною прихованістю.

Розглянемо міру структурної прихованості багаторівневого сигналу. Для кількісної оцінки структурної прихованості можна використовувати логарифмічну міру (ентропійну еквівалентність) – кількість біт, що необхідне для кодування множини допустимих комбінацій:

$$S_{\text{бтр}} = \log_2(A_q(L, d_0)). \quad (3.14)$$

У найпростішому випадку без обмеження на d_0 : $S_{\text{бтр}} = L \log_2 M$. Якщо накладається мінімальна відстань, тоді

$$S_{\text{бтр}} \leq \log_2 \left(\frac{M^L}{V_M(L, t)} \right) = S_{\text{бтр}} = L \log_2 M - S_{\text{бтр}} = L \log_2 V_M(L, t). \quad (3.15)$$

Розглянемо наступні чисельні приклади для оцінки множини формування сигнальних конструкцій якщо $L = 16$:

- 1) при $M = 2$ отримуємо $N = 65536$; $I = 16$;
- 2) при $M = 4$ отримуємо $N = 4,29 \times 10^9$; $I = 32$;
- 3) при $M = 8$ отримуємо $N = 2,81 \times 10^{14}$; $I = 48$.

Отже, можна зробити висновок, що той самий приріст довжини в бітах можна отримати або збільшенням L у двійковому випадку, або збільшенням M при фіксованому L . Результати розрахунків показників багаторівневого сигналу в залежності від для різних значень M і L при фіксованих значеннях d_0 представлено в табл. 3.2. На Залежність структурної прихованості представлена залежність структурної прихованості $S_{\text{бтр}}$ від кількості рівнів M для різних L при фіксованому значенні $d_0 = 3$. Бачимо, що для фіксованої довжини L збільшення числа рівнів M експоненційно (3.1) збільшує повний простір кодових слів N і лінійно (у логарифмічному вимірі) зростає інформаційний вміст I . Це створює можливість підвищення структурної прихованості, тобто,

чим більша кількість допустимих комбінацій, тим вища складність для аналізу. Ведення вимоги щодо мінімальної кодової відстані d_0 для забезпечення необхідного рівня завадостійкості суттєво скорочує реальний розмір множини допустимих кодів, про що свідчать розрахунки у табл. 3.2. Практично це означає необхідність компромісу при виборі M і L так, щоб при заданому d_0 отримати достатній рівень прихованості $S_{\text{бтр}}$, враховуючи апаратні та каналні обмеження на передаваний сигнал. Для забезпечення високого рівня прихованості при великих значеннях d_0 доцільно використовувати динамічну зміну множин кодових конструкцій для різних сеансів передавання інформації.

Непозиційне кодування [4, 29, 33] передбачає формування кодових комбінацій не за рахунок позицій імпульсів, а через використання вагових коефіцієнтів, тривалостей чи інших параметрів сигналів. Одним із прикладів є таймерне кодування, коли тривалості імпульсів кратні базовому часовому елементу Δ . Цей параметр обмежує мінімальну енергетичну відстань між дозволеними сигнальними конструкціями. Всупереч методу поелементного кодування, за якого мінімальна енергетична відстань визначається найквістовим елементом, у запропонованих конструкціях мінімальна відстань між ними в декілька разів менше «елемента Найквіста» $\Delta = t_0/s$; $s \in 1, 2, \dots, k$ – ціле число.

Отже, саме введення цього елемента дає змогу при обмеженій довжині кодового слова збільшувати число реалізацій. Сам елемент розраховується із забезпеченням доцільної ймовірності приймання одного кодового слова замість переданого на інтервалах «хорошого» стану каналу модулі Гільберта.

Іншим параметром таймерного кодування є мінімальна відстань між суміжними значущими моментами модуляції реалізованого кодового слова, тобто значення d_0 [51] має нижню границю, яка дорівнює найквістовому елементу):

$$\tau_{ci} \geq s\Delta + i\Delta; \quad i \in 0, 1, 2, \dots, z - \text{ціле число.} \quad (3.16)$$

Таблиця 3.2 – Розрахунки структурної прихованості для різних значень M і L при фіксованих значеннях d_0

M	L	$N = M^L$	$S_{\text{бтр}}$ при $d_0 = 3$	$S_{\text{бтр}}$ при $d_0 = 5$
2	8	256	4,83	2,79
2	16	65 536	11,91	8,90
2	32	4 294 967 296	26,96	22,95
4	8	65 536	11,36	7,89
4	16	4 294 967 296	26,39	21,86
4	32	$1,8447 \times 10^{19}$	57,40	51,84
8	8	16 777 216	18,17	13,52
8	16	$2,8147 \times 10^{14}$	41,18	35,45
8	32	$2,8128 \times 10^{28}$	88,19	81,42
16	8	4 294 967 296	25,08	19,35
16	16	$1,8447 \times 10^{19}$	56,09	49,27
16	32	$3,4028 \times 10^{38}$	119,09	111,23

Перший доданок умови (3.16) обмежує мінімальний часовий інтервал імпульсу таймерного сигналу, тобто елемент Найквіста $t_0 = s\Delta$. Доданок $i\Delta$ свідчить про збільшення значення τ_{ci} у порівнянні з найквістовим елементом t_0 . При заданих обмеженнях є можливість сформулювати наступну кількість сигнальних конструкцій [51]:

$$N_p = C_{ms-i(s-1)}^i \rightarrow \frac{[ms-i(s-i)]!}{i!(ms-i)!}, \quad (3.17)$$

де i – кількість заданих імпульсів таймерного сигналу на інтервалі m найквістових елементів. Наприклад, для $m = 8$ і $s = 7$ при синтезі сигнальної конструкції з 3-х інформаційних імпульсів $i = 3$ є можливість отримати наступну кількість таймерних сигналів $N_p = C_{56-3(7-1)}^3 = C_{38}^3 = \frac{38!}{3! \dots 35!} = 8436$, що у 33 рази більше кількості сигнальних конструкцій при $m = 8$, тобто $2^8 = 256$. Завдяки першому доданку (3.17) ТСК виключається можливість створення

власних міжсимвольних завад [51]. В табл. 3.3 за допомогою виразу (3.17) виконано розрахунок кількості реалізацій в залежності від значень $i \in 1 \div 6$, $s \in 2 \div 8$ і $m \in 4 \div 10$.

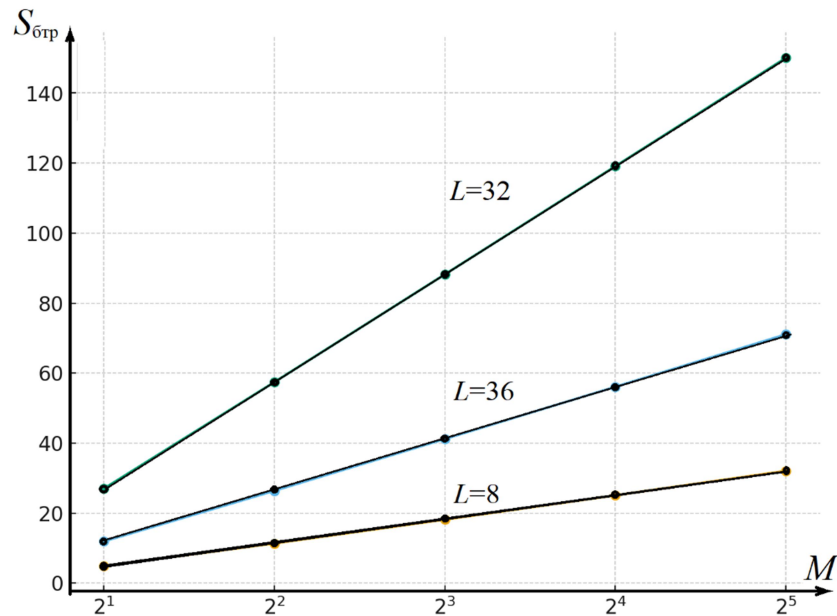


Рисунок 3.1 – Залежність структурної прихованості $S_{\text{бтр}}$ від кількості рівнів M для різних L і $d_0 = 3$

Аналіз табл. 3.3 свідчить, що за умови:

- 1) $m \geq 4$ і $i \geq 2$ для $s \geq 4$ кількість реалізацій більше $N_p > 2^m$;
- 2) $m_1 = 4$ і $m_2 = 5$ для $s \geq 3$ кількість реалізацій для $m = 5$, $N_p(5)$ майже вдвічі більше від $N_p(4)$;
- 3) $m \geq 5$ відношення кількості реалізацій при збільшенні інтервалу сигнальної конструкції з $T_c = mt_0$ до $T_c = (m + 1)t_0$ відповідає нерівностям:

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} < 2 \text{ при } i < 3; \quad (3.18)$$

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} > 2 \text{ при } i \geq 3; \quad (3.19)$$

Таблиця 3.3 – Кількість реалізацій таймерних сигналів в залежності від m , s та i

$\begin{smallmatrix} m \\ s \end{smallmatrix}$	4	5	6	7	8	9	10
$i = 1$							
2	7	9	11	13	15	17	19
3	10	13	16	19	22	25	28
4	13	17	21	25	29	33	37
5	16	21	26	31	36	41	46
6	19	25	31	37	43	49	55
7	22	29	36	43	50	57	64
8	25	33	41	49	57	65	73
$i = 2$							
2	15	28	45	66	91	120	153
3	28	55	91	136	190	253	325
4	45	91	153	231	325	435	561
5	66	136	231	351	496	666	861
6	91	190	325	496	703	946	1225
7	120	253	435	666	946	1275	1653
8	153	325	561	861	1225	1653	2145
$i = 3$							
2	10	35	84	165	286	455	680
3	20	84	220	455	816	1330	2024
4	35	165	455	969	1771	2925	4495
5	56	286	816	1771	3276	5456	8436
6	84	455	1330	2925	5456	9139	14190
7	120	680	2024	4495	8436	14190	22100
8	165	969	2925	6545	12341	20825	32509
$i = 4$							
2	1	15	70	210	495	1001	1820
3	1	35	210	715	1820	3876	7315
4	1	70	495	1820	4845	10626	20475
5	1	126	1001	3876	10626	23751	46376
6	1	210	1820	7315	20475	46376	91390
7	1	330	3060	12650	35960	82251	163185
8	1	495	4845	20475	58905	135751	270725
$i = 5$							
2	0	1	21	126	462	1287	3003
3	0	1	56	462	2002	6188	15504
4	0	1	126	1287	6188	20349	53130
5	0	1	252	3003	15504	53130	142506
6	0	1	462	6188	33649	118755	324632
7	0	1	792	11628	65780	237336	658008
8	0	1	1287	20349	118755	435897	1221759
$i = 6$							
2	0	0	1	28	210	924	3003
3	0	0	1	84	924	5005	18564
4	0	0	1	210	3003	18564	74613
5	0	0	1	462	8008	54264	230230
6	0	0	1	924	18564	134596	593775
7	0	0	1	1716	38760	296010	1344904

4) побудувавши залежності числа реалізацій від збільшення однієї зі змінних за сталих значень інших можна констатувати їх нелінійність.

5) для всіх значень $m > 4$ при $s > 4$ отримуємо $N_p \gg 2^m$.

Апроксимуючі рівняння мають наступний вигляд:

1) для $N_p = f(S)$:

$$\begin{aligned} i = 2 \quad \sqrt[2]{N_p(i, m, S)} &= 1,416S + 1,045; \\ N_p(i, m, S) &= (1,416S + 1,045)^2; \end{aligned} \quad (3.20)$$

$$\begin{aligned} i = 3 \quad \sqrt[3]{N_p(i, m, S)} &= 0,554S + 1,053; \\ N_p(i, m, S) &= (0,554S + 1,053)^3; \end{aligned} \quad (3.21)$$

2) для $N_p = f(m)$:

$$\begin{aligned} i = 2 \quad \sqrt[2]{N_p(i, m, S)} &= 3,536m - 6,02; \\ N_p(i, m, S) &= (3,536m - 6,02)^2; \end{aligned} \quad (3.22)$$

$$\begin{aligned} i = 3 \quad \sqrt[3]{N_p(i, m, S)} &= 2,759m - 7,23; \\ N_p(i, m, S) &= (2,759m - 7,23)^3. \end{aligned} \quad (3.23)$$

З метою оцінки ефективності таймерного кодування порівняємо результати передавання інформації для двох методів кодування на основі: РЦК з реєстрацією у середині посилання посилки t_0 ; таймерних сигналів. Аналіз порівняння результатів передавання комбінацій при ТСК і РЦК з урахуванням довжин їх побудови показує наступне:

1) енергетична відстань для ТСК визначається зоною у сім разів меншою відносно РЦК, тобто $\Delta = t_0/7$;

2) ймовірності помилкового приймання комбінації різняться не суттєво;

3) у випадках, коли T_c (ТСК) $<$ T_c (РЦК), імовірність помилкового приймання при ТСК може бути меншою порівняно з РЦК.

З урахуванням отриманих даних в табл. 3.4 відзначимо, що за приблизно рівних ймовірностей приймання РЦК і ТСК число реалізацій таймерних сигналів на заданому інтервалі n в десятки разів більше, ніж при РЦК. Наприклад, при $s = 3$, $i = 3$ на інтервалі $T_c = 10t_0$ можна отримати $N_p = 22100$ ТСК (табл. 3.3), а при РЦК – $N_p = 1024$ ($2^{10} = 1024$). Коефіцієнт збільшення дорівнює 21,58 (22100:1024). Якщо ж формувати конструкції з п'яти інформаційними ЗММ ($i = 5$), то на інтервалі $T_c = 10t_0$ можлива реалізація 658008 КС (табл. 3.3), тобто коефіцієнт збільшення відносно РЦК буде дорівнювати 642,5.

Таблиця 3.4 – Вплив довжини конструкції на якість передавання

РЦК				ТСК: $s=7; i=3$			
n	$N_{\text{пер}}$	$N_{\text{пом}}$	$P_{\text{п}}$	n	$N_{\text{пер}}$	$N_{\text{пом}}$	P_n
20	100000	700	$7 \cdot 10^{-3}$	17	100000	11,50	$11,5 \cdot 10^{-3}$
40	100000	1500	$15 \cdot 10^{-3}$	$n=33$	100000	1620	$16,2 \cdot 10^{-3}$
10	100000	720	$7,2 \cdot 10^{-3}$	$n=9$	100000	104	$7,1 \cdot 10^{-4}$

Таке збільшення числа реалізацій суттєво збільшує пропускну здатність каналу (навіть при алфавіті каналу $a = 2$). При чому граничне значення пропускну здатності буде визначатися виразом:

$$C_{\text{макс}} = \frac{\log_2 N_{\text{п}\Sigma}}{T_{\text{ск}}}, \quad (3.24)$$

де $T_{\text{ск}}$ – часовий інтервал сигнальної конструкції в числі найквістових елементів, $N_{\text{п}\Sigma}$ – загальна кількість реалізацій, які використовуються з урахуванням кількості ЗММ – i .

3.3. Оцінка структурної прихованості та мінімальної кодової відстані при виборі реалізацій таймерних сигналів методом перебору

Потенційна структурна прихованість (3.1) визначається через кількість можливих сигнальних конструкцій N_p , що використовуються для передавання інформаційних символів. Розглянемо можливість збільшення кількості реалізацій N_p шляхом застосування непозиційного таймерного кодування в межах часового інтервалу побудови сигнальних конструкцій $T_c = nt_0$, де n – кількість елементів Найквіста. Важливим базовим елементом побудови таймерних сигналів є часовий інтервал Δ , за допомогою якого задається тривалість імпульсів за наступним виразом: $t_c = t_0 + k\Delta$, де $k = 0, 1, 2, \dots, s \cdot (n - 2)$. Непозиційність таймерних сигналів пояснюється тим, що тривалості імпульсів t_c кратні базовому елементу Δ , який задається співвідношенням $\Delta = t_0/s$ (де $s = 1, 2, 3, \dots, l$ – цілі числа) і повинні задовольняти умові Найквіста [51]:

$$t_c \geq t_0 = \frac{1}{\Delta F}. \quad (3.25)$$

Кількість Δ на інтервалі t_0 визначається параметром $s = t_0/\Delta$. Такий алгоритм формування імпульсів зменшує енергетичну відстань між сигнальними конструкціями і визначається величиною $\Delta < t_0$. Це дозволяє на інтервалі T_c збільшити в порівнянні з РЦК кількість таймерних сигналів [32]:

$$N_{p\text{ТСК}} = [ns - i(s - 1)]!/i! (ns - is)!, \quad (3.26)$$

де: i – кількість інформаційних моментів модуляції.

Комбінований вибір параметрів n , s і i дозволяє створювати різні ансамблі таймерних сигналів, які будуть відрізнятися структурою і кількістю $N_{p\text{ТСК}}$. Враховуючи особливості побудови ТСК слід відзначити, що збільшення $N_{p\text{ТСК}}$

шляхом зменшення часового інтервалу Δ призводить до погіршення завадостійкості передачі, але при цьому структурна прихованість зростає. Такі властивості таймерного кодування потрібно враховувати при виборі параметрів ТСК.

У табл. 3.5 наведено кількість ТСК $N_{\text{рТСК}}$, що сформовані методом підбору в залежності від значень параметрів n , s , i для кодової відстані $d_0(\Delta) = 1, 2, \dots, 9$. Бачимо, що для комбінації параметрів $n = 7$, $i = 3$, $s = 5$ і $d_0(\Delta) = 1$ отримуємо $N_{\text{рТСК}}=1771$ (табл. 3.5, №1), проте як для РЦК кількість сигнальних конструкцій значно менше $N_{\text{рРЦК}}=2^7=128$. Значено більшу кількість таймерних сигналів $N_{\text{рТСК}} = 2925$ можливо отримати при $s = 6$ (табл. 3.5, № 3), що зменшує тривалість базового елемента Δ . Подальше збільшення кількості можливих комбінацій ТСК досягається шляхом розширення інтервалу їх побудови T_p . Це дозволяє розташувати більше імпульсів із різними часовими зсувами, що безпосередньо підвищує кількість сигнальних конструкцій $N_{\text{рТСК}}$. Значення $N_{\text{рТСК}}=3276$ (табл. 3.5, №4) можна отримати для $n = 8$, $i = 3$, $s=5$ і $d_0(\Delta) = 1$. Як бачимо з табл. 3.5, зі збільшенням кодової відстані $d_0(\Delta)$ кількість можливих реалізацій $N_{\text{рТСК}}$ зменшується. За умови виконання нерівності:

$$d_0(\Delta) \geq 2 \quad (3.27)$$

стає можливою реалізація завадостійкого кодування на основі таймерного кодування шляхом розмежування дозволених та недозволених комбінацій сигнально-кодових конструкцій. Для оцінки параметра $d_0(\Delta)$ запропоновано використовувати кодовий критерій Хеммінга, модифікований з урахуванням кількості часових інтервалів Δ , які відповідають елементам ТСК:

$$d_0(\Delta) = \sum_{j=1}^W x_j \oplus z_j \quad (3.28)$$

де x_j і z_j – відповідні часові реалізації двох сигнальних конструкцій ("0" або "1") по елементам Δ , $W = n \cdot s$ – кількість елементів Δ на інтервалі часу T_c .

На рис. 3.2 представлені приклади реалізації ТСК з різними значеннями кодової відстані $d_0(\Delta)$ при параметрах $n = 7, i = 3, s = 5$:

- 1) ТСК-1: $t_{c1}=5\Delta, t_{c2}=6\Delta, t_{c3}=24\Delta$;
- 2) ТСК-2: $t_{c1}=6\Delta, t_{c2}=10\Delta, t_{c3}=19\Delta$;
- 3) ТСК-3: $t_{c1}=10\Delta, t_{c2}=17\Delta, t_{c3}=8\Delta$.

Таблиця 3.5 – Кількість ТСК в залежності від параметрів n, s, i і $d_0(\Delta)$, що отримані методом підбору

№	Параметри ТСК			Кількість ТСК $N_{\text{ТСК}}$ в залежності від $d_0(\Delta)$								
	N	i	s	1	2	3	4	5	6	7	8	9
1	7	3	5	1771	891	248	146	79	53	36	28	22
2	7	3	6	2925	1469	395	231	121	85	53	44	31
3	7	3	7	4495	2255	591	344	176	121	76	60	44
4	8	3	5	3276	1638	438	252	133	91	59	47	33
5	8	3	6	5456	2736	714	408	316	146	94	70	50
6	8	3	7	8436	4218	1079	615	316	212	137	102	75

Для цих комбінацій отримано такі значення кодової відстані:

- 1) $d_0(\Delta)=6$ для ТСК-1 і ТСК-2;
- 2) $d_0(\Delta)=21$ для ТСК-1 і ТСК-3;
- 3) $d_0(\Delta)=15$ для ТСК-2 і ТСК-3.

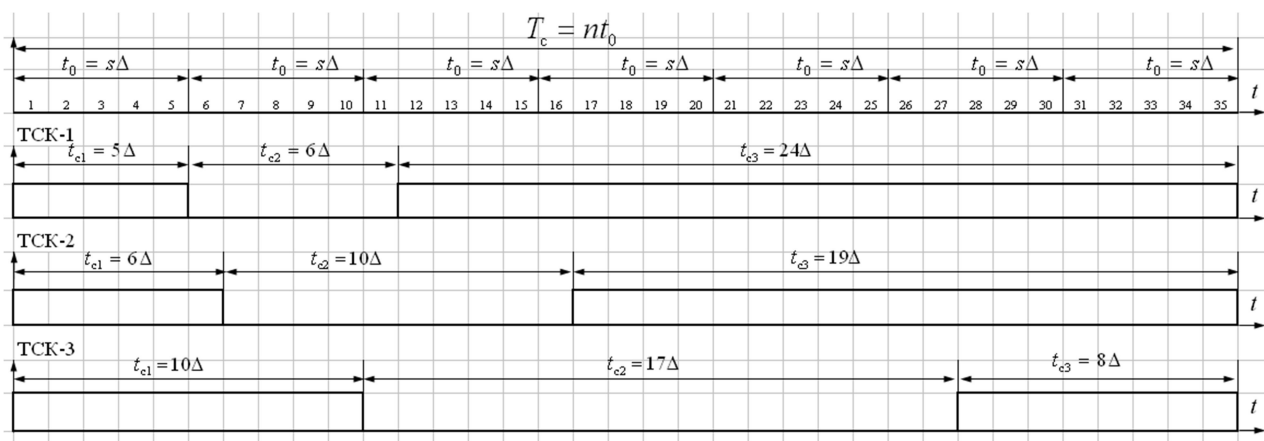


Рисунок 3.2 – Реалізації таймерних сигналів з різними значеннями $d_0(\Delta)$

Як показано у табл. 3.5, зі збільшенням кодової відстані $d_0(\Delta)$ кількість можливих реалізацій $N_{\text{ТСК}}$ зменшується. Відповідно до (3.1), це призводить до зниження показника структурної прихованості сигнальних конструкцій $S_{\text{ТСК}}$ (рис. 3.2). Отже, між структурною прихованістю $S_{\text{ТСК}}$ та завадостійкістю існує суперечливий взаємозв'язок, який необхідно враховувати при розробці алгоритмів обміну даними в системах зв'язку. Для компенсації зменшення значення показника $S_{\text{ТСК}}$ у випадку зростання $d_0(\Delta)$ пропонується застосовувати різні множини сигнальних конструкцій $\{N_{\text{ТСК}_i}(d_0(\Delta))\}$, кожна з яких характеризується певним значенням кодової відстані. При цьому інтегральний показник структурної прихованості визначається як

$$S_{\text{ТСК}} = \log_2 \left(\sum_{z=1}^L N_{\text{ТСК}_i}(d_0) \right), \quad (3.29)$$

де L – кількість множин ТСК. Отже, вибір параметрів n , s та i безпосередньо впливає як на завадостійкість, так і на структурну прихованість сигнальних конструкцій.

3.4. Вплив рівнянні якості при таймерному кодуванні на рівень структурної прихованості та завадостійкості

З технічної точки зору, для реалізації таймерного кодування доцільно застосовувати рівняння якості Захарченко М.В. [32], яке дозволяє формувати множину дозволених комбінацій:

$$\sum_{k=1}^i A_k x_k \equiv 0 \pmod{A_0} \quad (3.30)$$

де $A_k (k = 1, i)$ – вагові коефіцієнти, що утворюють систему простих чисел, A_0 – модуль, x_k – номери відділків ЗММ імпульсів t_{ci} .

Якщо сигнальна конструкція задовольняє умові (3.30), вона вважається дозволеною. Це дозволяє здійснювати відбір із загальної множини кодових комбінацій лише тих, які відповідають вимогам завадостійкості. У табл. 3.6 наведено мінімальні

кодові відстані $d_0=2\div 4$, отримані для значень параметрів A_0, A_1, A_2, A_3 . Усі множини допустимих таймерних сигналів відрізняються між собою кількістю комбінацій, структурою побудови та значенням кодової відстані.

Таблиця 3.6 – Коефіцієнти рівняння якості для формування дозволених таймерних сигналів

№	d_0	A_0	A_1	A_2	A_3
1	4	19	2	3	7
2	2	7	2	3	5
3	2	11	2	3	7
4	3	13	2	3	7
5	-	17	2	3	7

У табл. 3.7 наведено приклади вибірок $N_{\text{рТСК}}$ дозволених кодових комбінацій із кодовою відстанню $d_0(\Delta) = 4$, що формуються на основі рівняння якості при параметрах $A_0=19, A_1=2, A_2=3, A_3=7$, а також різних значеннях параметрів побудови n, s, i . Додатково, у табл. 3.7 наведені реалізації ТСК зі значеннями $d_0(\Delta) \geq 5$, які отримані шляхом відбору із початкової множини $d_0(\Delta) = 4$. Це демонструє можливість формування більш захищених сигнально-кодових конструкцій шляхом поетапного збільшення кодової відстані. Як бачимо з табл. 3.6, кількість дозволених ТСК, що задовольняють рівнянню якості (3.30) для заданих параметрів $A_k (k = 1, i)$ і A_0 , є суттєво меншою порівняно з повним перебором усієї множини сигнально-кодових конструкцій (3.26). Наприклад, для параметрів $n = 7, i = 3, s = 5$ та кодової відстані $d_0(\Delta) = 4$ кількість допустимих реалізацій становить лише $N_p=93$ (табл. 3.6, № 1) із загального числа можливих комбінацій $N_{\text{рзаг}}=1771$, тоді як при повному переборі кількість реалізацій дорівнює $N_p=146$ (табл. 3.5, № 2). Подальше збільшення кодової відстані призводить до ще більшого скорочення допустимої множини. Так, при $d_0(\Delta)=5$ кількість реалізацій зменшується до

$N_p=37$ (табл. 3.5, № 1), у той час як при повному переборі цей показник дорівнює $N_p=79$ (табл. 3.5, № 1). На рис. 3.3 представлена залежність структурної прихованості $S_{\text{ТСК}}$ від $d_0(\Delta)$ для ТСК, що отримані методом підбору.

Таблиця 3.7 – Вибірki реалізацій ТСК по рівнянню якості з $A_0=19$, $A_1=2$, $A_2=3$, $A_3=7$ і $n, s, i, d_0(\Delta)$

№	Параметри ТСК			N_p	Вибірki дозволених ТСК в залежності від $d_0(\Delta)$					
	m	i	S		4	5	6	7	8	9
1	7	3	5	1771	93	37	27	24	15	13
2	7	3	6	2925	154	59	43	41	23	19
3	7	3	7	4495	236	88	68	58	34	29
4	8	3	5	3276	173	65	52	40	27	22
5	8	3	6	5456	288	106	82	68	42	35
6	8	3	7	8436	444	156	123	98	60	49

Збільшенням параметра $d_0(\Delta)$ кількість можливих реалізацій зменшується, що відповідно до (3.1) призводить до зниження структурної прихованості сигнально-кодових конструкцій. Суперечливий характер співвідношення показників прихованості та завадостійкості необхідно враховувати під час розроблення алгоритмів обміну даними у системах зв'язку. Вочевидь, що для компенсації зниження показника $S_{\text{ТСК}}$ доцільним є використання змінних множин сигнально-кодових конструкцій із заданими параметрами $\{N_{\text{ТСК}_i}(d_0)\}$ для різних сеансів передавання конфіденційної інформації, тоді:

$$S_{\text{ТСК}} = \log_2 \left(\sum_{z=1}^L N_{\text{ТСК}_i}(d_0) \right). \quad (3.31)$$

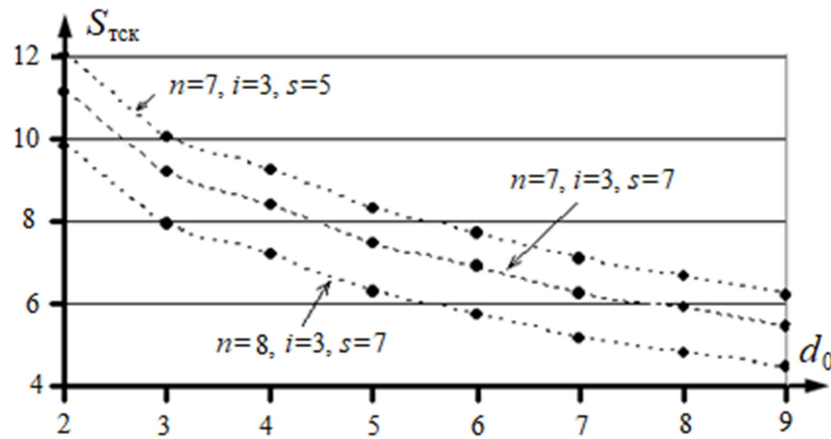


Рисунок 3.3 – Залежність структурної прихованості S_{TCK} від $d_0(\Delta)$ для ТСК, що отримані методом підбору

Отже, параметри n , s та i можуть одночасно впливати як на завадостійкість, так і на структурну прихованість сигнально-кодових конструкцій. Шляхом варіювання параметрів рівняння якості A_0 , A_1 , A_2 , A_3 можна синтезувати множини сигнальних конструкцій, які відрізняються за кількістю комбінацій і мінімальною кодовою відстанню d_0 . Це створює передумови для розроблення алгоритмів підвищення структурної прихованості з урахуванням вимог до завадостійкості. З однієї сторони, рівняння якості (3.31) є ефективним інструментом для реалізації завадостійкого таймерного кодування. З іншого сторони, при цьому зменшується кількість допустимих комбінацій, що необхідно враховувати при розробленні алгоритмів підвищення структурної прихованості передавання інформації на основі таймерних сигналів. Метод повного перебору (3.26) дає змогу максимально використовувати усе множинне сигнальних конструкцій для формування допустимих комбінацій, тому їхня кількість завжди більша, ніж при застосуванні рівняння якості (3.31). Рівняння якості (3.31) є більш зручним засобом реалізації завадостійкого таймерного кодування. Водночас слід враховувати, що кількість дозволених комбінацій при цьому виявляється меншою, ніж у випадку повного перебору (табл. 3.7), що безпосередньо впливає на показник структурної прихованості. Синтезування різних множин сигнальних конструкцій досягається шляхом варіювання параметрів A_0 , A_1 , A_2 ,

A_3 у межах допустимих значень. Використання об'єднаної (сумарної) множини комбінацій у такому випадку дозволяє: підвищити рівень структурної прихованості відповідно до виразу (3.29); забезпечити необхідний рівень достовірності передачі інформації; зберегти баланс між кількістю реалізацій та завадостійкістю кодування.

3.5. Захист інформації на основі j -кратного повторення надлишкових таймерних сигналів

У даному дослідженні розглянута можливість підвищення рівня захищеності конфіденційної інформації в однобічних системах передавання шляхом збільшення кількості реалізацій СКК на основі таймерного кодування при обмеженому часовому інтервалі, що забезпечує перевагу порівняно з традиційними методами РЦК. Забезпечення достовірного приймання інформації в конфіденційних системах зв'язку залишається однією з ключових задач інформаційної безпеки. Відомо, що достовірність приймання в системах зв'язку [51, 60] зазвичай досягається шляхом зниження ефективної швидкості передавання, що пов'язано з додаванням надлишкових перевірочних символів при використанні завадостійкого коду або шляхом багаторазового повторення переданих повідомлень. Коригувальна здатність таких методів обумовлена досягненням необхідної мінімальної кодової відстані d_0 . При використанні розрядно-цифрового кодування рівень надлишковості, необхідний для забезпечення заданої достовірності, як правило, визначається без урахування поточного стану дискретного каналу, якість якого може змінюватися. У результаті цього протягом більшості часу експлуатації ІКС фактична надлишковість на один інформаційний символ перевищує мінімально необхідний рівень, що знижує загальну ефективність передачі. Метою цього дослідження є оцінка підвищення рівня захищеності передаваної інформації в ІКС шляхом застосування надлишкових таймерних сигналів [51].

У якості сигнальних структур, здатних перетворювати надлишок достовірності в підвищену пропускну здатність каналу, запропоновано використання ТСК. Формування таких конструкцій ґрунтується на застосуванні базового часового елемента Δ , тривалість якого може змінюватися з метою не лише регулювання енергетичної відстані між сусідніми конструкціями, а й забезпечення необхідного рівня їх роздільності. Це, у свою чергу, дає можливість керувати кількістю реалізацій сигнальних комбінацій у межах обмеженого часовим інтервалом T_c , що є критично важливим для досягнення високої ефективності та надійності передавання інформації. Значення $T_c = mt_0$ визначає часовий інтервал побудови таймерних сигналів, де t_0 – тривалість бітового елемента РЦК (інтервал Найквіста), m – кількість елементів t_0 . При побудові ТСК потрібно враховувати наступне [32]:

1) кодова відстань між ЗММ сигнальних конструкцій таймерних сигналів не менше інтервалу Найквіста, тобто $t_0 = 1/\Delta F$, де ΔF – смуга пропускання каналу зв'язку, але й не кратна йому;

2) кодова відстань кратна часовому відрізку $\Delta = t_0/s$ ($s \in 2, 3, \dots k$), а відстань між ЗММ визначається як: $\tau_c = t_0 + \Delta \times l$ ($l \in 0, 1, 2, 3, \dots$).

Такий алгоритм побудови таймерних сигналів з обмеженням відстані τ_c забезпечує усунення міжсимвольних спотворень між сигнальними конструкціями. Значення s показує, наскільки зменшуються Δ по відношенню до t_0 . Приклади побудови таймерних сигналів з кількістю переходів $i = 3$ надано на рис. 3.4.

Кількість дозволених таймерних сигналів з різним числом переходів i на інтервалі побудови сигнальних конструкцій $T_c = mt_0$ визначається за формулою [51, 60]:

$$N_{p \text{ ТСК}} = \sum_{i=1}^n \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [(n \cdot s) - [(s-1) \cdot i] - i]!}. \quad (3.32)$$

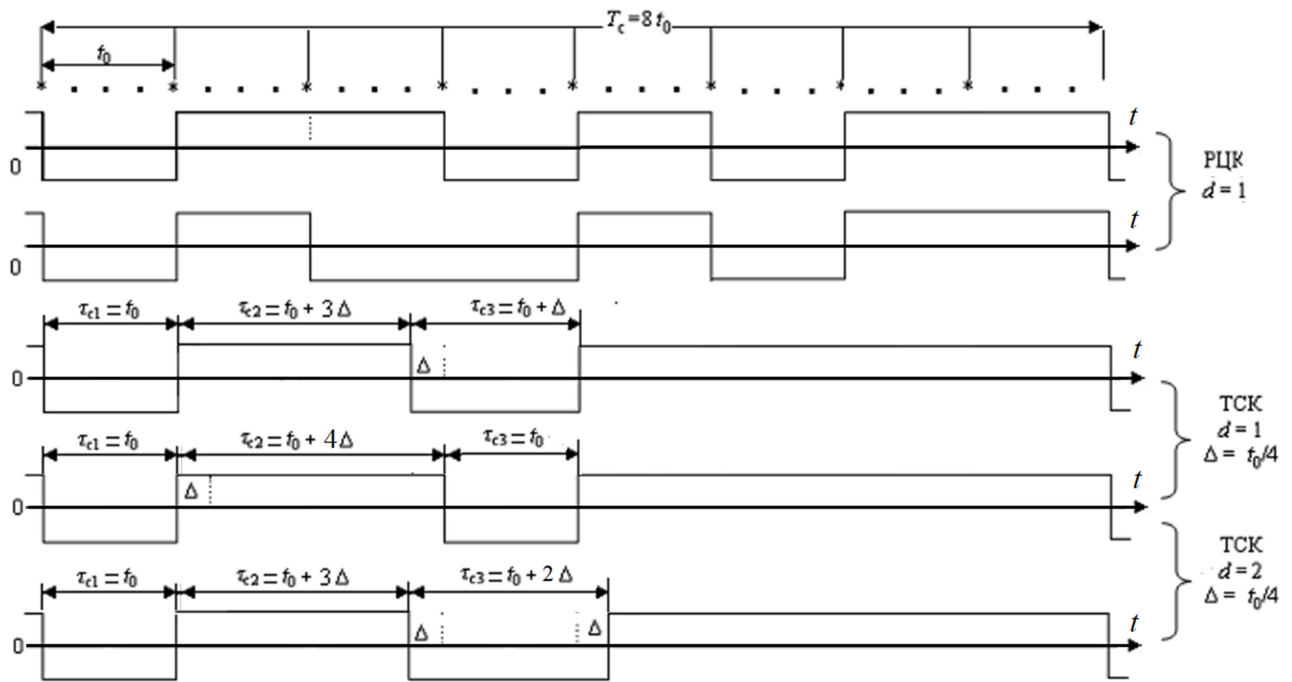


Рисунок 3.4 – Побудова таймерних сигналів з кількістю ЗММ $i = 3$

Розрахункові значення кількості комбінацій $N_{p_тск}$ у залежності від s и m надано в табл. 3.7. Бачимо, що збільшення показника s дозволяє збільшити число реалізацій ТСК при фіксованому значенні m . Розглянемо ймовірності помилкового $P_{п}$ і вірного прийому $P_{в}$ сигнальних конструкцій з числом ЗММ від 1 до m , які розраховуються за наступними формулами [51, 60]:

$$P_{п} = 1 - \left[2\Phi \left(2h/s \right) \right]^i, \quad (3.33)$$

$$P_{в} = 1 - P_{п}, \quad (3.34)$$

де $\Phi \left(2h/s \right)$ – функція Крампа, i – кількість ЗММ.

На основі (3.33) та (3.34) можна зробити висновок, що зменшення енергетичної відстані між сигнальними конструкціями шляхом збільшення s впливає на якість реєстрації на прийомальній стороні. При виборі оптимального значення параметра s слід враховувати фактичне співвідношення

сигнал/шум h у каналі, оскільки саме воно визначає можливість забезпечення необхідної якості передачі.

Отже, збільшення кількості можливих реалізацій сигнальних конструкцій [32, 43] у межах заданого інтервалу часу безпосередньо призводить до зростання пропускну здатності бінарного каналу порівняно з класичним завадостійким кодуванням на основі РЦК [51]. Це означає, що з'являється можливість гнучкого обміну між якістю передавання та швидкістю, тобто підвищення темпу передавання інформації за рахунок допустимого зниження завадостійкості.

Таблиця 3.8 – Кількість реалізацій при ЗММ $i = 3$

$\begin{matrix} s \\ m \end{matrix}$	4	5	6	7	8	9	10
4	35(2)	165(9)	455(24)	969(51)	1771(93)	2925(154)	4495(237)
5	56(3)	286(15)	816(43)	1771(93)	3276(172)	5456(287)	8436(444)
6	84(4)	455(24)	1330(70)	2925(154)	5456(287)	9139(481)	14190(747)
7	120(6)	680(36)	2024(107)	4495(237)	8436(44)	14190(747)	22100(1163)
8	165(9)	969(51)	2925(154)	6545(344)	12341(650)	20825(1096)	32509(1711)
9	220(12)	1330(70)	4060(214)	9139(481)	17296(910)	29260(1540)	45760(2408)

Крім того, використання розширеного ансамблю реалізацій ТСК відкриває принципово нові можливості для організації ефективного процесу виявлення та виправлення помилок. У цьому випадку вся множина сигнальних конструкцій ділиться на дві підмножини: дозволені, які можуть бути використані для передачі інформації, та недозволені, які трактуються як помилкові. Отже, формується надлишковий код на основі ТСК, однак на відміну від традиційних методів РЦК, реалізація такого підходу не вимагає введення додаткових надлишкових елементів у вигляді перевірних бітів. Вибір підмножини дозволених сигнальних конструкцій здійснюється відповідно до рівняння якості (3.35), яке задає баланс між кількістю можливих реалізацій, завадостійкістю та ймовірністю помилки. Це дозволяє оптимізувати систему з

урахуванням конкретних умов передачі та вимог до швидкості й надійності каналу.

Таким чином, застосування ТСК у поєднанні з принципом формування надлишкових кодів без додаткових контрольних символів відкриває перспективний напрям розвитку сучасних систем зв'язку, особливо в умовах обмежених ресурсів та впливу інтенсивних завад. Рівняння якості описується наступним виразом [51]:

$$A_1x_1 + A_2x_2 + \dots + A_nx_n = Z \pmod{A_0}, \quad (3.35)$$

де A_i – коефіцієнти, за допомогою яких забезпечуються певні відстані між дозволеними ТСК, x_i – число елементів Δ на інтервалі часу τ_{ci} .

У табл. 3.9 в дужках наведено число дозволених реалізацій у разі використання ТСК в режимі виявлення або виправлення помилок. За допомогою значень коефіцієнтів A_i визначається кодова відстань між таймерними сигналами. Кодова відстань d яка дорівнює сумі різниць тривалості відповідних інформаційних відрізків τ_i у значеннях елементів Δ [39]:

$$d = \sum_{S=1}^i (\tau_{S1} - \tau_{S2}), \quad (S \in 1; 2; \dots i), \quad (3.36)$$

де: τ_{S1} , τ_{S2} – тривалості s -го часових інтервалів імпульсів першої або другої сигнальної конструкції.

За допомогою такого алгоритму побудови ТСК виникає можливість створювати різну надлишковість на заданому інтервалі T_c , що дозволяє виявляти або виправляти помилки. При цьому виникає завдання пошуку відповідних вагових коефіцієнтів A_k ($k = 1, \dots, i$) та модуля A_0 для виразу $\sum A_i x_i = 0 \pmod{A_0}$ для забезпечення заданих властивостей коду. Синтез таймерних кодів ґрунтується на двох основних теоретичних положеннях. Перша з них – Теорема 12 [51] – формулює критерії, за яких можлива побудова кодів, здатних забезпечувати лише виявлення помилок у процесі

передавання інформації. Друга – Теорема 13 [51] – виступає основою для розробки більш складних таймерних кодів, що дозволяють не лише виявляти, а й виправляти помилки. Відповідно до Теорема 12, умови синтезу коду виконуються у випадку, коли коефіцієнти рівняння (3.35) мають такі значення, що:

$$\begin{aligned} A_k &= (e_0 + 1)^{k-1}; \quad k \in \{1 \dots i\} \\ A_0 &= (e_0 + 1)^i, \end{aligned} \quad (3.37)$$

то помилки кратності меншої або рівної i величиною $[-e_0; e_0]$ виявляються з імовірністю 1. Відповідно до теорема 13, якщо коефіцієнти A_k рівняння (3.37) визначено таким чином, що [52]:

$$A_k = (2e_0 + 1)^{k-1}; \quad k \in \{1 \dots i\}, \quad A_0 = (2e_0 + 1)^i, \quad (3.38)$$

то всі помилки кратності, що не перевищує i , та величиною у діапазоні $[-e_0; e_0]$ гарантовано виявляються з імовірністю, що дорівнює одиниці. Інакше кажучи, такий синтез таймерних кодів забезпечує абсолютну завадостійкість відносно виявлення помилок в межах заданих параметрів. Для перевірки висунутих теоретичних припущень було виконано два статистичних експерименти [60], спрямовані на оцінювання характеристик реального каналу під час передавання сигналів із використанням різних типів кодування РЦК і ТСК. У першому дослідженні здійснювалася передача 8-бітових кодових слів через канали у смузі пропускання $\Delta F = 1300$ Гц зі швидкістю 1000 біт/с із використанням модему на основі ЧМ. Під час експерименту отримано такі результати:

- 1) загальна кількість переданих кодових комбінацій – 360 000;
- 2) кількість помилково прийнятих кодових комбінацій – 364;
- 3) розподіл за кратністю помилок у спотворених словах:
 - 1-кратні – 244 випадки;
 - 2-кратні – 102 випадки;

- 3-кратні – 16 випадків;
- 4-кратні – 1 випадок;
- 5-кратні – 1 випадок.

Отримані статистичні дані дали змогу розрахувати основні параметри каналу. Ймовірність помилкового прийому кодового слова склала $P_{н.кс} = 1,01 \times 10^{-3}$, а ймовірність спотворення окремого біта дорівнює $P_{\epsilon} = 1,75 \times 10^{-4}$. Для характеристики групування помилок було визначено коефіцієнт α , який обчислюється за співвідношенням:

$$\hat{I} = \frac{\ln \bar{t}}{\ln n}, \quad (3.39)$$

де $\bar{t}$ – середня кількість спотворених елементів у помилкових кодових словах, n – довжина кодового слова.

У наведеному експерименті середня кількість спотворених бітів становила $\bar{t} = 1,38$, що відповідає коефіцієнту групування $\alpha = 0,16$. Отже, експериментально підтверджено наявність помилок, які виникають не лише незалежно, але й у вигляді згрупованих спотворень для даного каналу.

Для реалізації виправлення помилок у системі пропонується використання передачі з J -кратним повторенням таймерних сигналів. Особливість ТСК полягає в тому, що вони здатні не лише виявляти помилки, але й здійснювати їхнє коригування. Це дозволяє застосовувати мінімально можливе значення параметра J , не знижуючи надійність передавання. У процесі J -го приймання рішення щодо правильності тієї чи іншої сигнальної конструкції приймається на основі сумісного аналізу рівняння якості (3.37), що виконується паралельно з використанням J -декодерів ТСК. Враховуючи той факт, що кожен із декодерів має здатність виправляти помилки, можна вважати, що з певною ймовірністю хоча б один із них правильно відновить хоча б одну з прийнятих J -реалізацій сигнальної конструкції. Такий підхід дозволяє істотно скоротити необхідну кількість

повторів. У найпростішому випадку, коли $J = 2$, уже досягається гарантоване підвищення достовірності приймання. Звідси впливає перша задача експерименту – перевірка ефективності декодування при двократному повторі ТСК. Разом із тим, наявність у реальному каналі явища групування помилок свідчить про те, що передавання однакових сигналів послідовно без часових інтервалів не забезпечить достатньої ефективності. Для підвищення завадостійкості доцільно застосовувати метод декореляції помилок, тобто передавати повтори однакових сигнальних конструкцій через певні часові інтервали. Це дозволяє знизити ймовірність того, що всі копії сигналу потраплять до однієї пачки помилок. Відповідно, виникає друга задача експерименту – дослідити статистичний розподіл інтервалів безпомилкового приймання та визначити оптимальні параметри для організації повторів із часовим рознесенням.

У рамках другого експерименту було здійснено передавання коригуючих таймерних сигналів тим самим каналом з обмеженою смугою частот. Для побудови використовувався таймерний код, який відповідає умові якості (3.35) за наступних значень коефіцієнтів A_i : $A_1 = 2$; $A_2 = 3$; $A_3 = 7$; $A_0 = 19$. Сформовані таким чином таймені сигнали забезпечують можливість виявлення помилок величиною до 2Δ та їх виправлення в межах 1Δ . У роботі [60] було показано, що за умови використання 256 реалізацій кодових слів із трьома ЗММ, які задовольняють вимогу (3.35) при $s=7$, достатнім є інтервал реалізації інформаційної частини кодової конструкції $T_c = 7,5t_0$. На такому інтервалі можливо реалізувати $256 \times 19 = 4864$ простих ТСК. Фрагмент результатів передавання 2×10^6 кодових конструкцій, що відповідають умові (3.37), наведено нижче:

- 1) вірно прийнято кодових слів – 1 984 263;
- 2) кількість комбінацій зі зміщенням на величину $\Theta = \Delta$ – 12 704;
- 3) кількість комбінацій зі зміщенням на величину $\Theta = 2\Delta$ – 85;
- 4) кількість комбінацій зі зміною числа ЗМВ – 2948.

Слід зазначити, що комбінації зі зміщенням на $\Theta=2\Delta$, а також ті, що мають зміну числа ЗМВ, не підлягають виправленню обраним таймерним кодом. У табл. 3.9 наведені варіанти прийняття рішень під час декодування ТСК. Для глибшої оцінки ефективності було проведено аналіз статистики помилок із врахуванням безпомилкового інтервалу L ($L = 0,1, \dots, 9$) між двома хибними кодовими комбінаціями. Узагальнені результати подано в табл. 3.10, де:

- 1) $N_{\text{пом1}}$ – кількість помилкових пар ТСК через інтервал L до декодування;
- 2) $P_{\text{пом1}}$ – ймовірність появи такої пари до декодування;
- 3) $N_{\text{пом2}}$ – кількість помилкових пар після роботи декодера;
- 4) $P_{\text{пом2}}$ – ймовірність появи пари після декодування.

Таблиця 3.9 – Результати декодування при двократному передаванні ТСК

№	Вид помилкової ТСК відповідної пари		Рішення при декодуванні
1	1 Δ	0 Δ	Виправлення
2	1 Δ	1 Δ	Виправлення
3	1 Δ	2 Δ	Виправлення
4	1 Δ	Дроблення	Виправлення
5	2 Δ	0 Δ	Виправлення
6	2 Δ	2 Δ	Виявлення
7	2 Δ	Дроблення	Виявлення
8	Дроблення	0 Δ	
9	Дроблення	Дроблення	Виявлення

Аналіз даних табл. 3.10 показує, що найменша ймовірність виникнення помилки для пари ТСК, яка становить $1,6 \cdot 10^{-5}$, досягається за умови використання інтервалу декореляції $L = 4$. Проте подальше збільшення значення інтервалу призводить до нестабільності результатів – спостерігається дрейф у бік як збільшення, так і зменшення значення ймовірності. Це свідчить

про те, що інтервали більші за $L = 4$ не є ефективними для забезпечення надійності системи.

Враховуючи характер розподілу інтервалів між спотвореними кодовими словами та параметри цього розподілу, можна стверджувати, що ймовірність появи двох або навіть трьох сусідніх спотворених конструкцій є досить високою. Тому як оптимальний захисний інтервал повторення було обрано інтервал, що відповідає $J = 4$ кодовим словам.

З експериментальних результатів також випливає, що ймовірність виникнення спотвореного кодового слова з фіксованим числом ЗММ дорівнює $P_{n(i=3)} = \frac{2948}{2000000} = 1,474 \times 10^{-3}$. Це значення є вищим за відповідну ймовірність $P_{п.кс}$, що отримується при використанні розрядно-цифрового кодування. Така різниця пояснюється тим, що у випадку РЦК аналізувались лише ті кодові слова, які були прийняті з помилками у середній точці сигналу, тоді як у даному випадку враховувались також слова, де число ЗМВ відхилялося від заданого значення (3.37), або ж їхня позиція у часовій шкалі не збігалася з переданими.

Таблиця 3.10 – Статистичні дані розподілу помилкових пар ТСК

L	0	1	2	3	4	5	6	7	8	9
Обидва кодові слова пари мають зміщення на величину $\Theta \geq 1\Delta$ чи дроблення										
$N_{\text{пом1}}$	310	136	149	143	139	162	119	121	115	124
$P_{\text{пом1}}$	0,00031	0,00014	0,000149	0,000143	0,000139	0,000162	0,000119	0,000121	0,000115	0,0001
Обидва кодові слова пари мають зміщення на величину $\Theta \geq 2\Delta$ чи дроблення										
$N_{\text{пом2}}$	186	42	59	49	16	64	18	28	19	10
$P_{\text{пом2}}$	0,00019	4,2E-05	0,000059	0,000049	0,000016	0,000064	0,000018	0,000028	0,000019	1E-05

Знаючи кількість ЗМВ, що змістилися при прийманні на величину 1Δ , а також загальну кількість ЗМВ у правильно прийнятих кодових словах, можна оцінити середньоквадратичне відхилення для випадку «хорошого» стану каналу [61] $\left(\frac{1,5\Delta}{\delta}\right) - \Phi\left(\frac{0,5\Delta}{\delta}\right) = \frac{51 \times 2}{(90000-13)3} = 2 \times 10^{-3}$, де: $\Phi(z)$ – інтеграл

ймовірностей. При $\Delta = 0,142t_0$ ($s = 7$) ($s = 7$) значення параметру δ не перевищує $\delta = 0,02t_0$. У такому випадку ймовірність зміщення одного ЗМВ у «хорошому» стані каналу на величину $\Theta \geq 2\Delta$ обчислюється як $P_1 = P_{\Theta \geq 2} = 2 \left[0,5 - \Phi \left(\frac{1,5\Delta}{\delta} \right) \right] = 2 \left[0,5 - \Phi \left(\frac{1,5 \times 0,142}{0,021} \right) \right] \leq 10^{-10}$. Для випадків зміщення двох або трьох ЗМВ у межах інтервалу $\frac{3}{2}\Delta > \Theta > \frac{1}{2}\Delta$ ймовірності дорівнюють:

$$P_2 = P_{2(\frac{3}{2}\Delta > \Theta > \frac{1}{2}\Delta)} = C_3^2 \left[\Phi \left(\frac{1,5\Delta}{\delta} \right) - \Phi \left(\frac{0,5\Delta}{\delta} \right) \right]^2 = 1,2 \times 10^{-7};$$

$$P_3 = P_{3(\frac{3}{2}\Delta > \Theta > \frac{1}{2}\Delta)} = \left[\Phi \left(\frac{1,5\Delta}{\alpha} \right) - \Phi \left(\frac{0,5\Delta}{\alpha} \right) \right]^3 < 10^{-11}.$$

На основі цих даних визначимо ймовірність невиявленої помилки при двократному повторенні ТСК: $P_{\text{НП2}} = P_1P_1 + P_1P_2 + P_1P_3 + P_2P_2 + P_2P_3 + P_3P_3$. Оскільки найбільший внесок у результат робить ймовірність P_2 , іншими складовими можна знехтувати. Таким чином, остаточна оцінка дорівнює $P_{\text{НП2}} \approx P_2P_2 = 1,44 \cdot 10^{-14}$. Отримані результати підтверджують високу ефективність використання методу J -кратного повторення для підвищення завадостійкості системи. У табл. 3.11 наведено узагальнені результати експериментальної перевірки різних алгоритмів роботи одnobічної системи передачі з повторенням. Результати аналізу ефективності двократного повторення надлишкового ТСК можна підсумувати наступним чином:

1) експериментально встановлено, що найближчий безпомилковий інтервал між двома помилковими кодовими комбінаціями становить $L = 4$, що забезпечує мінімальну ймовірність помилки пари ТСК;

2) у межах запропонованого алгоритму декодування всі помилкові ТСК були виявлені, більшість з них виправлені, хоча певна частина пар кодових комбінацій підлягала стиранню;

3) теоретичні розрахунки показали, що ймовірність невиявленої помилки при двократному повторенні ТСК є на вісім порядків меншою, ніж для коду РЦК (15,7) за тієї ж кодової швидкості R ;

4) висока ефективність виявлення помилок підтверджує доцільність застосування цього алгоритму передачі ТСК у системах із зворотним зв'язком.

Таблиця 3.11 – Розрахункові значення показників ефективності системи зв'язку при передаванні ТСК і РЦК

Параметри сигнальних конструкцій	ТСК $J=2$	РЦК (15,7) $d=5$	РЦК (23,12) $d=7$	РЦК (73,37) $d=11$
R	0,53	0,47	0,52	0,51
$P_{\text{НП2}}$	$1,44 \cdot 10^{-14}$	$1,72 \cdot 10^{-06}$	$2,32 \cdot 10^{-07}$	$1,248 \cdot 10^{-14}$

Висновки

У третьому розділі було проведено системний аналіз та дослідження застосування непозиційних таймерних сигналів як основи для забезпечення захисту інформації від несанкціонованого доступу. Показано, що структурна прихованість сигналів є важливим додатковим механізмом інформаційної безпеки, який доповнює традиційні криптографічні методи.

1. Надано оцінку позиційному та непозиційному кодуванню формування сигнальних конструкцій для забезпечення показника структурної прихованості. Встановлено, що двійкові позиційні сигнали мають обмежену потенціальну можливість щодо формування сигнальних конструкцій із складною структурою і, тому, можуть забезпечувати захист інформації переважно за рахунок криптографії. Використання багаторівневих та таймерних сигналів дозволяють суттєво розширити простір допустимих кодових комбінацій, підвищуючи структурну прихованість.

2. Досліджено можливості позиційного та непозиційного кодування по синтезу достатньо великого простору кодових комбінацій, що забезпечує підвищення структурної прихованості. Показано, що при збільшенні кількості рівнів та довжини кодових комбінацій кількість можливих реалізацій експоненційно зростає. Виявлено суттєве обмеження простору сигнальних конструкцій у випадку вимоги на забезпечення мінімальної кодової відстані при завадостійкому кодуванні.

3. Проведено аналіз взаємозв'язку між структурною прихованістю та коригувальною здатністю таймерних сигнальних конструкцій залежно від параметрів їх побудови. Встановлено, що збільшення кодової відстані d_0 зменшує кількість допустимих кодових комбінацій, що, у свою чергу, знижує структурну прихованість сигнальних конструкцій. Суперечливий характер співвідношення показників структурної прихованості та завадостійкості необхідно враховувати під час розроблення алгоритмів обміну даними в системах зв'язку.

4. Виконано оцінку структурної прихованості та мінімальної кодової відстані для таймерних сигналів з використанням рівняння якості Захарченка. Рівняння якості є більш зручним засобом реалізації завадостійкого таймерного кодування. Водночас слід враховувати, що кількість дозволених комбінацій при цьому виявляється меншою, ніж у випадку повного перебору, що безпосередньо впливає на показник структурної прихованості. Використання рівняння якості дозволяє керовано змінювати співвідношення між завадостійкістю та структурною прихованістю. Зміна параметрів рівняння A_0 , A_1 , A_2 , A_3 дає можливість синтезувати множини кодових комбінацій з різними характеристиками, що важливо для адаптивного формування захищених каналів зв'язку.

5. Проаналізовано застосування j -кратного повторення надлишкових таймерних сигналів. Доведено, що введення контрольованої надлишковості дозволяє підвищити як завадостійкість, так і прихованість сигналів завдяки розширенню множини допустимих реалізацій.

Отже, результати досліджень у розділі показали, що використання непозиційних таймерних сигнальних конструкцій дає можливість синтезувати багаторівневі захищені канали зв'язку з керованим балансом між завадостійкістю та структурною прихованістю, що підвищує загальну ефективність захисту інформації від несанкціонованого доступу.

4 ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕГРОВАНИХ МЕТОДІВ ПЕРЕТВОРЕННЯ ДАНИХ

У розділі обґрунтовано підхід до підвищення захищеності передавання інформації шляхом поєднання трьох методів перетворення даних: стохастичного шифрування, завадостійкого та таймерного кодування. Запропоновано модель багаторівневого захисту, в основі якої – використання трьох послідовних перетворювачів: внутрішнього (реалізує стохастичне шифрування для забезпечення інформаційної прихованості), проміжного (використовує блокове кодування для підвищення завадостійкості) та зовнішнього (реалізує таймерне кодування для структурної прихованості та компенсації надлишковості). Показано доцільність урахування ентропії джерела повідомлень при формуванні шифрограми, що підвищує ефективність шифрування. Обґрунтовано перспективність застосування інтегрованого підходу до захисту даних у сучасних інформаційно-комунікаційних системах, зокрема в умовах впливу засобів радіоелектронної боротьби.

4.1. Обґрунтування комбінованих методів шифрування і кодування

Упродовж розвитку криптографії та теорії передачі інформації дослідники неодноразово вдавалися до поєднання засобів криптографічного захисту та захисту від помилок, розуміючи, що ці два напрями взаємодоповнюють один одного – перший забезпечує конфіденційність, другий – цілісність і достовірність. Одна з перших у світі систем захищеного голосового зв'язку SIGSALY (США) [61, 62], що поєднувала шифрування сигналу та корекцію помилок було запропонована ще в 1943 році. Ця система використовувала шифрування сигналу за допомогою одноразових шумових записів. В каналі з радіозв'язком корекція помилок було реалізовано шляхом введення надлишковості при передаванні кодових блоків.

Американський криптоаналіз радянських шифрограм у проєкті VENONA показав, що використання одноступеневих шифрів без додаткового кодування робить систему вразливою [62]. Це стало стимулом для подальшого розвитку поєднання криптографії та кодування для мінімізації витоку інформації навіть за умови часткового розкриття ключів. У системах захищеного зв'язку НАТО та СРСР активно використовувались блокові шифри (наприклад, DES) спільно з циклічними надлишковими кодами (CRC, BCH) для забезпечення достовірної передачі даних на зашумлених каналах, включаючи супутникові й радіорелейні лінії [52]. У таких системах шифрування захищало вміст повідомлення, а коди виправлення помилок відновлювали спотворену інформацію у спотворених кодових блоках. З розвитком цифрових стандартів мобільного зв'язку (GSM, CDMA) було впроваджено багаторівневі моделі обробки даних, у яких дані шифрувалися (алгоритм A5/1, A5/3) та передавалися з використанням канального кодування (конволюційні, турбо-коди), а також піддавалися модуляції та розширення спектру, що забезпечувало маскування їх у частотному спектрі [63].

Сучасні захищені протоколи (наприклад, TLS/SSL) функціонують переважно на мережних рівнях, що передбачає поєднання шифрування (AES, RSA) із виявленням помилок і спотворень (HMAC, CRC) та фактично утворює багаторівневий механізм захисту [63]. Отже, наданий огляд показує, що комбінування методів шифрування і кодування є ефективним засобом у забезпеченні завадозахищеності передаваної інформації. Воно дозволяє досягти одночасного захисту від несанкціонованого доступу, помилок передачі та виявлення сигналу, що є критично важливим в умовах радіоелектронного протистояння.

Однією з ключових умов забезпечення ефективного захисту інформації в інформаційно-комунікаційних системах є реалізація багаторівневого підходу, який поєднує методи криптографічного шифрування та засоби завадостійкого кодування. Такий підхід дозволяє реалізувати одночасне забезпечення: конфіденційності; цілісності та достовірності; прихованості передачі.

Забезпечення конфіденційності за допомогою шифрування є ключовим компонентом комбінованого захисту інформації. Відповідно до класичної теорії Шеннона [66], конфіденційність визначається неможливістю статистичного або структурного аналізу шифрограми без знання ключа. Модель комбінованого захисту може бути представлена у наступному вигляді [49, 66, 67]:

$$Z = f(C_{\text{шифр}}, C_{\text{зк}}, \gamma, S), \quad (4.1)$$

де Z – загальний рівень захищеності, $C_{\text{шифр}}$ – криптографічна стійкість шифрування, $C_{\text{зк}}$ – здатність коду до виявлення/виправлення помилок, γ – відносна надлишковість (ресурсне навантаження), S – структурна/енергетична прихованість.

У класичному випадку для передавання повідомлення M використовується функція шифрування:

$$C = E_K(M), \quad (4.2)$$

де M – повідомлення, E_K – функція шифрування з ключем K , C – шифротекст.

Однак при передачі через канал із завадами, шифротекст може бути спотворений, і приймач отримає $C' \neq C$, що призводить до неможливості розшифрування повідомлення M . Тому вводиться процедура захисту від помилок через функцію завадостійкого кодування:

$$C_{\text{код}} = \text{Encode}(E_K(M)), \quad (4.3)$$

а приймач виконує декодування і розшифрування:

$$\hat{M} = D_K(\text{Decode}(C'_{\text{код}})), \quad (4.4)$$

де $\text{Encode}(\cdot)$ – функція завадостійкого кодування, $\text{Decode}(\cdot)$ – функція декодування, D_K – розшифрування з тим самим ключем K , $C'_{\text{код}}$ – спотворене кодоване повідомлення.

Імовірність помилки в кодовому блоку без завадостійкого кодування [51]:

$$P(\geq 1, n) \approx 1 - (1 - p_0)^n \quad (4.5)$$

де p_0 – ймовірність помилки в одному біті, n – довжина шифртексту.

Імовірність помилки в кодовому блоку з використанням завадостійкого кодування в комбінованій системі [51]:

$$P(\geq t, n) \approx \sum_{i=t+1}^n \binom{n}{i} p_0^i (1 - p_0)^{n-i}, \quad (4.6)$$

де t – кратність виправлення помилок.

Ентропійна оцінка захищеності повідомлення полягає в наступному. У разі використання стохастичного шифрування, де одному повідомленню відповідає декілька можливих шифртекстів, ентропія повідомлення після шифрування зростає. Згідно з концепцією Шеннона [65] необхідно, щоб:

$$H(K) \geq H(M) \quad (4.7)$$

де $H(K)$ – ентропія ключа, $H(M)$ – ентропія повідомлення.

Стохастичне шифрування, як складова комбінованої системи, дозволяє підвищити рівень конфіденційності шляхом генерування великої кількості рівноймовірних шифрограм навіть для одного і того ж повідомлення. Це підвищує ентропію переданого сигналу та ускладнює його розшифрування навіть при частковому перехопленні.

При ідеальному шифруванні отримуємо наступне:

$$H(C) = H(K) + H(M) \quad (4.8)$$

де $H(C)$ – ентропія шифрованого повідомлення.

При цьому забезпечується інформаційна прихованість, за умови великих просторах ключів та ймовірнісному виборі шифрограм. Шифрування забезпечує криптографічний захист від несанкціонованого доступу. Використання стохастичного шифрування (СШ) дозволяє кожному повідомленню відповідати безліч можливих шифрограм, що ускладнює криптоаналіз. Наприклад, при стохастичному шифруванні повідомлення з трьох символів може формувати до $M=2^3=8$ різних шифрованих комбінацій. Ентропія Шеннона використовується для оцінки потенціалу конфіденційності:

$$H(U) = -\sum_{j=1}^L p_j \cdot \log_2 p_j, \quad (4.9)$$

де p_j – ймовірність появи символу μ_j .

При однакових імовірностях $p_j = 1/L$, максимальна ентропія $H_{max} = \log_2 L$ визначає кількість випадкових бітів, необхідних для маскування повідомлення. Забезпечення цілісності та достовірності шляхом корекції помилок є ще однією критично важливою складовою багаторівневого захисту інформації. Ці характеристики гарантують, що приймач отримає саме те повідомлення, яке було передане, незважаючи на вплив випадкових або цілеспрямованих завад. Для цього використовуються різні засоби завадостійкого кодування, зокрема: циклічні коди, у тому числі коди Хеммінга; коди Ріда-Соломона; турбо-коди та LDPC. У межах комбінованої моделі захисту інформації корекція помилок виконує функцію забезпечення надійного відновлення переданих даних, компенсуючи вплив завад та атак. У поєднанні з шифруванням і таймерним кодуванням це створює комплексну модель цілісного захисту для інформаційно-комунікаційних систем. Ця умова виконується, наприклад, в одноразовому блокноті, але її практична реалізація потребує великих обсягів ключів [67]. Тому в комбінованих системах доцільним є використання псевдовипадкових генераторів, які забезпечують достатню ентропію при обмежених ресурсах.

Отже, поєднання шифрування та кодування дозволяє досягати одночасної конфіденційності шляхом шифрування та достовірності за допомогою коригувальних кодів, що особливо важливо в умовах радіоелектронного протистояння, де інформація може бути не лише перехоплена, а й спотворені. Конфіденційність як складова захищеності в багаторівневій системі досягається саме завдяки правильно підбраному шифруванню. Його поєднання з методами завадостійкого та таймерного кодування утворює цілісну модель захисту, в якій шифрування відповідає за інформаційну прихованість, кодування – за достовірність, а системи модуляції у поєднанні з таймерними сигналами та методами розширення спектра – за структурну прихованість. Схема багаторівневої комбінованої системи захисту інформації за допомогою різних методів перетворення даних наведена на рис. 4.1.

Можна запропонувати наступну модель оцінки ефективності багаторівневого захисту у вигляді комбінованого критерію

$$Z_{\text{зах}} = f(p_{0\text{д}}, H(C), S), \quad (4.10)$$

що залежить від трьох показників: імовірності помилкового біту після декодування $p_{0\text{д}}$, ентропії шифрованого повідомлення $H(C)$ та ступеня структурної прихованості $S = \log_2 N_p$. Максимізація $Z_{\text{зах}}$ можлива лише при одночасному врахуванні завадостійкості, прихованості та криптостійкості.

4.2. Структура захисту інформації з багатьма перетворювачами

У сучасних умовах дії засобів РЕБ ефективний захист інформації можливий лише при сумісному використанні шифрування та завадостійкого кодування. Додаткове використання процедури розширення спектра дозволяє реалізувати структурну та енергетичну прихованість, що ускладнює виявлення сигналу засобами радіотехнічної розвідки. Одночасно, застосування стохастичного шифрування забезпечує інформаційну непередбачуваність

переданого повідомлення, а блокові коди, наприклад, Хеммінга, Ріда-Соломона [50, 51] виконують функцію виявлення або виправлення помилок у спотворених кодових блоках в приймачі. Представлені на рис. 4.1 складові перетворення даних особливо важливі для реалізації інтегрованих систем захисту інформації, де внутрішній рівень забезпечує криптографічне перетворення, проміжний – завадостійке кодування, а зовнішній – структурну та енергетичну прихованість за допомогою певних методів формування шумоподібних сигналів [30, 68, 69]. В цьому аспекті узагальнена модель комбінованого захисту інформації [66] може бути доповнена системою модуляції, певним методом розширення спектра та має наступний вигляд:

$$Z_{\text{заг зах}} = f(C_{\text{шиф}}, C_{\text{зк}}, \gamma, S_{\text{мод}}, S_{\text{роз}}, S_{\text{ен}}), \quad (4.11)$$

де: $Z_{\text{заг зах}}$ – загальний рівень захищеності, $C_{\text{шиф}}$ – криптографічна стійкість шифрування, $C_{\text{зк}}$ – здатність коду до виявлення/виправлення помилок, γ – відносна надлишковість (ресурсне навантаження), $S_{\text{мод}}$ – структурна прихованість сигнальних конструкцій системи модуляції, $S_{\text{роз}}$ – структурна прихованість методу розширення спектра цифрового коду, $S_{\text{ен}}$ – енергетична прихованість сигнальних конструкцій в каналі.

Зростання ризиків НСД [70-72] потребує забезпечення більш високого рівня захисту переданої інформації, що обґрунтовує поєднання різних методів інформаційної безпеки. Традиційно використовуються криптографічні методи шифрування, які гарантують конфіденційність даних, проте сам по собі шифрований сигнал може бути виявлений та ідентифікований засобами радіотехнічної розвідки. З іншого боку, використання лише методів кодування не забезпечує необхідного рівня криптостійкості та секретності. Комбінування шифрування та кодування [49] дозволяє реалізувати багаторівневий підхід до захисту, де кожен рівень виконує певне завдання по забезпеченню перетворення даних: шифрування; завадостійке кодування; таймерне кодування. Шифрування забезпечує інформаційну прихованість, тобто

ускладнює доступність вмісту повідомлення для несанкціонованих осіб. Завадостійке кодування забезпечує достовірність передавання в умовах дії завад певного рівня. Таймерне кодування забезпечує структурну прихованість сигнально-кодових конструкцій, що ускладнює виявлення та аналіз сигналу. У даному дослідженні обґрунтовано, що комплексне застосування стохастичного шифрування, блокових кодів корекції помилок та таймерного кодування дозволяє не лише підвищити загальну захищеність системи, але й оптимізувати витрати енергетичних, частотних та інформаційних ресурсів каналу.

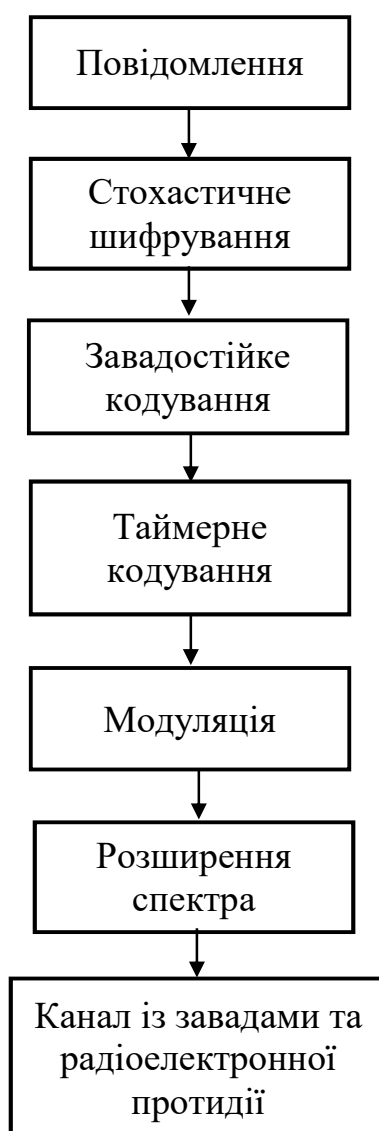


Рисунок 4.1 – Схема багаторівневої комбінованої системи захисту інформації за допомогою різних методів перетворення даних

Такий підхід дозволяє мінімізувати надлишковість, характерну для окремого застосування кожного методу, та досягти балансу між завадостійкістю, прихованістю та ефективністю передавання. Використання стохастичного шифрування [49] дозволяє формувати різні реалізації шифрованих комбінацій для одного й того ж повідомлення, що ускладнює криптоаналіз навіть за умови часткового перехоплення. Водночас, таймерне кодування дозволяє перетворити структуру сигналу таким чином, щоб змінити часові характеристики передачі, маскуючи інформаційні елементи та формуючи шумоподібні сигнали.

Таким чином, необхідність комбінування методів шифрування та кодування обумовлена наступними чинниками:

- 1) вимогами до багатовимірного захисту інформації (за критеріями завадостійкості, прихованості, достовірності);
- 2) підвищенням ефективності використання ресурсів каналу зв'язку;
- 3) адаптацією до змінних умов передачі та наявності загроз (динаміка РЕБ, НСД, електронного моніторингу);
- 4) забезпеченням стійкості системи до перехоплення, дешифрування та завад.

Доцільність побудови інтегрованої моделі захисту інформації ґрунтується на поєднанні шифрування, завадостійкого та таймерного кодування як базових елементів багаторівневої системи перетворення даних. Отже, для побудови ефективного багаторівневого захисту інформації в умовах високого рівня загроз запропоновано використовувати три взаємопов'язані перетворювачі (внутрішній, проміжний, зовнішній), кожен з яких виконує окрему функцію у процесі забезпечення конфіденційності, цілісності та достовірності інформації.

Внутрішній перетворювач реалізує базове шифрування, при якому використовується ключ або маска з високою ентропією. Основною метою шифрування є забезпечення конфіденційності інформації на першому етапі перетворення даних.

Проміжний перетворювач виконує виправлення помилок та формування надлишкових кодів. Для цього можуть використовуватися циклічні коди, у тому числі коди Хеммінга або інші кодекоригувальні методи [50, 51]. Основна метою завадостійкого кодування є забезпечення цілісності інформації під час передачі. Для оцінки здатності до корекції помилок використовується значення мінімальної кодової відстані d_{min} між сусідніми дозволеними кодовими комбінаціями. Також можливий варіант використання завадостійкого коду з додатковою функцією шифрування.

Зовнішній перетворювач використовується для маскуванню сигналу в каналі зв'язку, при якому забезпечується захист передаваних сигнальних конструкцій від виявлення та аналізу, наприклад, через спектральне розширення. Основна мета цього перетворення є підвищення стійкості до перехоплення в умовах РЕБ. На рис. 4.2 представлена структура схема передавача з багаторівневим захистом інформації на основі трьох перетворювачів, в який використовується наступне позначення:

- 1) X – вхідне повідомлення;
- 2) Π_1 – внутрішній перетворювач на основі певного криптографічного протоколу;
- 3) Π_2 – проміжний перетворювач з використанням завадостійкого коду, що призводить збільшення розміру кодових блоків шифрованого повідомлення на величину додаткові перевірочних елементів;
- 4) Π_3 – зовнішній перетворювач з певним видом модуляції з можливістю подальшого розширення спектра;
- 5) $S_{скк}$ – вихідний сигнал, який передається через канал зв'язку.



Рисунок 4.2 – Структура схема передавача з багаторівневим захистом інформації

Вочевидь, що зовнішній перетворювач Π_3 можна розділити на кілька складових, щоб детальніше показати різні можливості підвищення захисту інформації за допомогою сигнально-кодових конструкцій, для яких будуть притаманні властивості структурної та енергетичної прихованості. На рис. 4.3 представлена структура схема зовнішнього перетворювача Π_3 . Як бачимо з рис. 4.3 структура зовнішнього перетворювача Π_3 має додаткові блоки перетворення, які впливають на захист передованої інформації від засобів НСД та радіоелектронної розвідки.

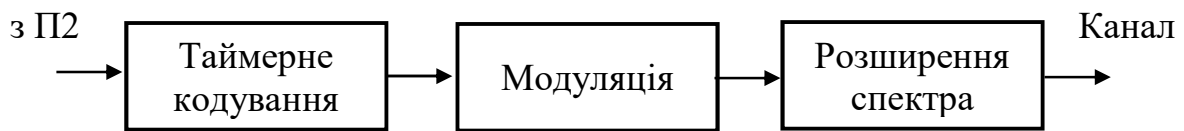


Рисунок 4.3 – Структура зовнішнього перетворювача Π_3

4.3. Взаємозв'язок між рівнями перетворення та критеріями захищеності

У запропонованій моделі багаторівневого захисту кожен рівень перетворення (внутрішній, проміжний, зовнішній) виконує специфічну функцію, що сприяє підвищенню загального рівня захищеності інформації при її передаванні [49]. Взаємозв'язок між рівнями можна представити у вигляді формалізованої моделі залежності критерію захищеності від характеристик кожного рівня:

$$Z_{\text{зах}} = f(Z_{\text{вн}}, Z_{\text{пр}}, Z_{\text{зов}}), \quad (4.12)$$

де $Z_{\text{зах}}$ – загальний критерій захищеності, $Z_{\text{вн}}$ – показник захищеності внутрішнього перетворення, $Z_{\text{пр}}$ – показник проміжного рівня перетворення, $Z_{\text{зов}}$ – показник зовнішнього перетворення.

Кожен з цих показників, у свою чергу, визначається як функція параметрів, що характеризують ефективність кодування, рівень ентропії та структурну складність перетворення:

$$Z_{\text{рів}} = f_e(p_{0\text{д}}, H(C), S, D_{\text{скл}}), \quad (4.13)$$

де $p_{0\text{д}}$ – ймовірність помилки після застосування завадостійкого кодування, $H(C)$ – ентропія результату перетворення, яка відображає рівень невизначеності, $D_{\text{скл}}$ – структурна складність схеми перетворення.

Для підвищення захищеності необхідно забезпечити таку комбінацію рівнів, при якій виконується умова:

$$\frac{dz_{\text{зах}}}{dz_{\text{рів}}} > 0 \text{ для кожного } Z_{\text{рів}} \in \{Z_{\text{вн}}, Z_{\text{пр}}, Z_{\text{зов}}\}. \quad (4.14)$$

Умова (4.14) означає, що зростання ефективності кожного окремого рівня повинно сприяти зростанню загального критерію захищеності.

4.4. Принципи формування шифрограм з варіативними комбінаціями

В основі внутрішнього перетворення лежить стохастичне шифрування, при якому один і той самий відкритий текст може відповідати кільком різним шифрограмам. Це досягається шляхом введення випадкових (або псевдовипадкових) елементів у процес шифрування. Такий підхід дозволяє значно підвищити ентропію шифрованого повідомлення та зробити його стійким до статистичного аналізу. Основні принципи статистичного шифрування побудовані на варіативності представлення шифрограм для повідомлення, ймовірнісне відображення та загальної функції шифрування [49].

Однією з ключових особливостей внутрішнього перетворювача, який реалізує стохастичне шифрування, є варіативність представлення вихідного

повідомлення. Це означає, що для одного і того ж вхідного повідомлення M формується множина шифрограм $\{C_1, C_2, \dots, C_n\}$, які є статистично різними, але при цьому дозволяють здійснити однозначне розшифрування. При цьому для кожного відкритого символу $x_i \in X$ існує множина допустимих комбінацій шифрування $C_i = \{c_{i1}, c_{i2}, \dots, c_{im}\}$, з яких обирається один випадково згідно з заданим розподілом імовірностей. Варіативність досягається шляхом використання випадкових параметрів у процесі шифрування. Формально, шифрування можна представити у вигляді функції:

$$C_i = E(M, K, R_i), \quad (4.15)$$

де M – вхідне повідомлення (наприклад, бітова послідовність), K – ключ шифрування, R_i – випадковий вектор або шумовий параметр, який змінюється при кожному шифруванні, C_i – результат шифрування при використанні випадкового вектору R_i .

Такий підхід дозволяє реалізувати невизначеність шифрограми, що суттєво підвищує криптостійкість: навіть при однаковому повідомленні та ключі, але різних R_i , шифрограми будуть різні. Це ускладнює проведення атак типу «обраного відкритого тексту». Загальний вигляд стохастичного шифратора можна подати як:

$$C = S_{\text{стат}}(M, K, R), \quad (4.16)$$

де: $S_{\text{стат}}$ – функція стохастичного перетворення.

Для кількісної оцінки варіативності доцільним є використання показника ентропії множини шифрограм:

$$H(C) = - \sum_{i=1}^n p(C_i) \cdot \log_2 p(C_i), \quad (4.17)$$

де $p(C_i)$ – імовірність появи конкретної шифрограми при заданому повідомленні M . Також варіативність стохастичного шифрування можна оцінити за допомогою умовної ентропії:

$$H(C|X) = -\sum_{i=1}^n \sum_{j=1}^{m_i} p_{ij} \log_2 p_{ij}. \quad (4.18)$$

При цьому, чим вищим є значення умовної ентропії $H(C|X)$, тим менш детермінованим є процес і результати шифрування. Ймовірнісне відображення статистичного шифрування можна відобразити наступним чином:

$$P(C_i = c_{ij} | x_i) = p_{ij}, \quad \sum_{j=1}^m p_{ij} = 1 \quad (4.19)$$

де p_{ij} – імовірність вибору конкретного представлення c_{ij} для відкритого символу x_i . Отже, використання статистичного шифрування дозволяє згенерувати велику кількість варіантів шифрування при фіксованому повідомленні та ключі, що значно ускладнює криптоаналітичні атаки на основі спостереження.

4.5. Вплив структури алфавіту і ймовірностей на ентропію

Структура алфавіту та розподіл ймовірностей появи символів у шифрограмі мають безпосередній вплив на ступінь прихованості переданої інформації. Згідно з формулою Шеннона [65], ентропія джерела дискретної інформації визначається як:

$$H = -\sum_{i=1}^{n_c} p_i \cdot \log_2 p_i, \quad (4.20)$$

де: n_c – кількість символів у алфавіті, p_i – імовірність появи символу i .

Максимальна ентропія досягається, коли розподіл імовірностей рівномірний, тобто $p_i = 1/n_c$. В цьому випадку:

$$H_{max} = \log_2 n_c. \quad (4.21)$$

Проте, при нерівномірному розподілі символів алфавіту ентропія зменшується. Системи шифрування, що динамічно змінюють структуру алфавіту та розподіл ймовірностей, можуть підвищити ентропію і знизити імовірність дешифрування шифрограми зломисником без знання ключа. Загальний принцип збільшення ентропії зашифрованого повідомлення полягає в наступному:

- 1) формується варіативний алфавіт A' , залежний від початкового алфавіту A та функції випадковості або генератора псевдовипадкових чисел;
- 2) значення p_i задаються або модулюються випадковим вектором $\vec{r}$, що змінюється з кожною сесією або блоком:

$$p'_i = f(p_i, r_i) \quad (4.22)$$

- 3) обчислюється поточна ентропія для кожного блоку, і контролюється, щоб вона не падала нижче заданого порогу H_{min} .

Отже, перетворення даних на основі шифрування має забезпечити вирівнювання частот розподілу символів шифротексту, щоб підвищити його ентропію до максимально можливого значення.

4.6. Інтеграція процесів шифрування та завадостійкого кодування

Підвищення прихованості та завадостійкості засноване на використанні трьох перетворювачів даних [49, 67]: внутрішнього, проміжного, зовнішнього. Внутрішній перетворювач використовує стохастичне шифрування для забезпечення інформаційної прихованості повідомлень. Перевагою цього

шифрування є можливість формування різного набору комбінацій шифрограми для однакового повідомлення. Проміжний перетворювач реалізує завадостійке кодування блоковим кодом для забезпечення розрахункової завадостійкості. Зовнішній перетворювач реалізує таймерне кодування для забезпечення структурної прихованості сигнальних конструкцій та компенсації надлишкових елементів при стохастичному шифруванні та завадостійкому кодуванні.

Для підвищення інформаційної прихованості передаваного повідомлення запропоновано при стохастичному шифруванні враховувати ентропію дискретного джерела інформації, що пов'язано з визначенням кількості випадкових комбінацій для кожного символу b_j алфавіту. Відповідно до виразу Шеннона ентропія для випадку подій з нерівноймовірними станами визначається формулою [56]:

$$H_{\text{HP}}(U) = -\sum_{j=1}^L p_j(u_j) \times \log_2 p_j(u_j). \quad (4.23)$$

Ентропія алфавіту обраної мови з урахуванням ймовірності появи символів у тексті становить $H_{\text{HP}}(U) = 4,42$. Ентропія для рівноймовірних символів алфавіту $H_p(U) = 5$. Вочевидь, що підвищити інформаційну прихованість при стохастичному шифруванні можливо при рівноймовірному законі появи випадкових комбінацій в шифрограмі повідомлення, тобто

$$H(U) \rightarrow H_p(U), \quad (4.24)$$

а також за умови, що

$$z \rightarrow \infty, \quad (4.25)$$

де $z = k + l$ – кількість двійкових елементів у випадковій кодової комбінації, k – кількість інформаційних елементів, l – кількість додаткових біт, які додаються до інформаційних елементів при стохастичному шифруванні.

Умову (4.24) можливо забезпечити, якщо кількість випадкових комбінацій вибирати з урахуванням ймовірності появи $p_j(u_j)$ кожного символу b_j використовуваного алфавіту. Умова (4.25) суттєво зменшує кодову швидкість, тому вибір значення z повинно бути обмежено з урахуванням вимог до швидкості передавання і інформаційної прихованості. При блоковому кодуванні довжина випадкової кодової комбінації збільшується на r елементів, тобто $n = k + l + r$, де r – кількість перевірочних елементів. Використання стохастичного шифрування зменшує кодову швидкість, так як

$$\gamma_{\text{кш}} = k/(k + l + r_2) < \gamma_{\text{к}} = k/(k + r_1), \quad (4.26)$$

де $\gamma_{\text{кш}}$ – кодова швидкість при спільному використанні стохастичного шифрування і блокового кодування; $\gamma_{\text{к}}$ – кодова швидкість блокового коду, r_1 – кількість перевірочних елементів для інформаційної комбінації з k елементів; r_2 – кількість перевірочних елементів для комбінацій із z елементів.

Вочевидь, що підвищити криптографічну стійкість повідомлення можна шляхом збільшення числа комбінацій в ансамблі C . Це означає, що $z = \lceil \log_2 M \rceil$ також збільшується. Для порівняльного аналізу в табл. 4.1 надана структура кодового блоку, що формується в залежності від варіанту кодування інформаційної послідовності k . Так для структури блоку $n = k + r_1$ забезпечується тільки завадостійке кодування (табл. 4.1 рядок №1). При стохастичному шифруванні ($n = k + l$) забезпечується тільки криптографічна стійкість. При комбінованому стохастичному шифруванні на основі РЦК із структурою блоку $n = k + l + r_2$ реалізується інтегрований захист каналу як від випадкових завад, так і НСД (табл. 4.1 № 3). Завадостійке кодування на основі ТСК дозволяє здійснити не тільки контроль по достовірності передавання інформації, а також – збільшити кодову швидкість $\gamma_{\text{к}}$. Пояснюється це тим, що інтервал побудови ТСК менше, ніж для завадостійких позиційних кодів, тобто $m_{\text{ТСК}} \leq k + r$ (табл. 4.1 № 5). При сумісному використанні стохастичного

шифрування та завадостійкого кодування комбінація позиційного коду $n = k + l + r_2$ замінюється на таймерну конструкцію.

Таблиця 4.1 – Варіанти формування кодових комбінацій при інтегрованому методі захисту інформації

№	Варіант кодування	Склад кодового блоку		
1	Завадостійке кодування на основі РЦК	K	r_1	-
2	Стохастичне шифрування	K	l	-
3	Стохастичне шифрування сумісно з блоковим завадостійким кодом	K	l	r_2
4	Завадостійке кодування на основі ТСК	$m_{\text{ТСК}} \leq k + r$		
5	Стохастичне шифрування на основі РЦК і двох ТСК	K	l	r_2
		$x_{\text{ТСК}}(t): m_{\text{ТСК}} < k + l + r_2$		
6	Стохастичне шифрування на основі РЦК і двох ТСК	K	l	r_2
		$m_{\text{ТСК1}} + m_{\text{ТСК2}} < k + l + r_2$		

Для підвищення криптографічної стійкості та збільшення кількості кодових реалізацій пропонується використовувати набір ТСК з двох комбінацій, одна з яких є дозволеною комбінацією, а друга може бути як дозволеною так і недозволеною та визначається за допомогою другої кодової книги. Сумісне використання блокового завадостійкого та таймерного кодування дозволяє збільшити завадостійкість, тому загальна ймовірність невиявленої помилки в кодовому блоці:

$$P_{\text{НП}} = P_{\text{НП-РЦК}} \times P_{\text{НП-ТСК}}, \quad (4.27)$$

де $P_{\text{НП-РЦК}}$ – ймовірність невиявленої помилки при блочному завадостійкому кодуванні; $P_{\text{НП-ТСК}}$ – ймовірність невиявленої помилки при таймерному кодуванні. При цьому інтервал побудови двох ТСК менше ніж для РЦК, тобто $m_{\text{ТСК1}} + m_{\text{ТСК2}} < k + l + r_2$, а мінімальна кодова відстань $d_0(\Delta)$ визначається обраним ансамблем дозволених комбінацій (табл. 4.1 № 5). Для оцінки ефективності стохастичного шифрування проведено імітаційне моделювання для двох варіантів реалізації перетворювача:

1) кількість випадкових кодових комбінацій є змінною величиною і визначається з урахуванням ймовірності появи символу алфавіту в тексті повідомлення;

2) однакова кількість випадкових кодових комбінацій для кожного символу алфавіту в тексті повідомлення.

Ефективність стохастичного шифрування була оцінена по дисперсії D_{xv} і D_{xc} відповідно для першого і другого варіантів в залежності від загальної кількості використовуваних випадкових комбінацій N_1 . У табл. 4.2 представлені результати досліджень для текстів різної довжини та n_2 . Бачимо, що при збільшенні розрядності кодування n_1 дисперсія D_{xv} для першого варіанту стохастичного шифрування зменшується значно швидше ($D_{xv} \rightarrow 0$), ніж D_{xc} для другого варіанту.

Таблиця 4.2 – Результати оцінок D_{xc} и D_{xv} для двох методів стохастичного шифрування

n_1	N_1	Текст розміру з 500 сторінок		Довільний текст з 10000 комбінацій		Текст пісні «Englishman in New York»	
		D_{xv}	D_{xc}	D_{xv}	D_{xc}	D_{xv}	D_{xc}
9	512	14 269 734,3	669 472 420,0	1 121,4	34 866,3	0,4	32,9
10	1024	4 408 878,1	124 230 180,0	22,7	8 772,3	0,1	7,8
11	2048	299 586,9	31 292 662,2	0,8	2 126,0	0,0	2,0
12	4096	40 566,6	8 025 058,9	0,3	531,7	0,0	0,5
13	8192	4 036,7	2 082 843,9	0,2	135,9	0,0	0,1
14	16384	316,2	543 439,8	0,1	33,8	0,0	0,0
15	32768	15,1	145 240,0	0,1	8,2	0,0	0,0
16	65536	1,4	40 101,8	0,0	1,8	0,0	0,0
17	131072	0,2	11 453,7	0,0	0,4	0,0	0,0

На виході стохастичного шифратора можна сформувати потік комбінацій з приблизно рівними ймовірностями появи, що ускладнює використання частотного тесту комбінацій шифрограми при дешифруванні у випадку її перехоплення. Також виявлено, що при стохастичному шифруванні великих обсягів текстів (500 сторінок) для досягнення умови $D_{xv} \rightarrow 0$ потребується

більша розрядність n_1 випадкових комбінацій. При цьому дисперсія $D_{xv} = 0,2$ буде отримана при розрядності $n_1 = 17$. Для тексту з 10000 комбінацій $D_{xv} = 0,2$ і $n_1 = 13$. Найкращий результат одержано при кодуванні невеликих текстів (пісня «Englishman in New York»): $D_{xv} = 0,1$ і $n_1 = 10$. Отже, запропонований метод комбінованого стохастичного шифрування може бути застосований для розробки реальних завадозахищених систем зв'язку, в яких вирішується задача підвищення прихованості і завадостійкості передавання секретної інформації.

4.7. Розробка методу формування простору випадкових комбінацій для системи статистичного шифрування

Основна ідея розробки алгоритму статистичного шифрування полягає у тому, що ймовірності появи шифрограм з виходу шифратора повинні прагнути до рівномірного закону. Передбачається, що це суттєво повинно ускладнити криптоаналіз шифрограм, а використання завадостійкого кодування знижує ймовірність помилок у кодових блоках повідомлення після їх декодування. Відомо, що при статистичному шифруванні отримані шифрограми з виходу шифратора мають надлишковість, які пов'язані з необхідністю збільшення простору випадкових комбінацій. Тому, для підвищення ефективності статистичного шифрування доцільно розглянути можливість зменшення надлишковості випадкових комбінацій при одночасному збереженні або навіть підвищенні рівня криптографічної стійкості. Це можливо за умови, що під час формування простору випадкових комбінацій E_i враховується ентропія дискретного джерела інформації [49, 66]. У випадку, коли символи на виході джерела інформації не підпорядковуються рівномірному закону розподілу, ентропія визначається виразом:

$$H_{NOL}(M) = - \sum_{j=1}^L p_j(m_j) \times \log_2 p_j(m_j), \quad (4.28)$$

де $p_j(m_j)$ – ймовірність появи символу m_j у повідомленні.

Хай ентропія для тексту з урахуванням ймовірності появи символів складає $H_{NUL}(M)=4,42$. З точки зору забезпечення криптостійкості статистичного шифрування бажаним є значення ентропії $H_{UL}(M)=5$, що свідчить про рівноймовірний розподіл символів у повідомленні. Звідси випливає перша умова підвищення криптографічної стійкості статистичного шифрування: комбінації, що застосовуються у просторі E_i для формування шифрограм, повинні з'являтися з рівноймовірним законом розподілу, тобто:

$$H_{NUL}(C) \rightarrow H_{UL}(C). \quad (4.29)$$

Також можна сформулювати другу умову підвищення криптографічної стійкості, яка пов'язана зі збільшенням надлишковості випадкових комбінацій з виходу шифратора, тобто

$$n = k + l \rightarrow \infty. \quad (4.30)$$

де n – загальна кількість розрядів випадкової комбінації, k – кількість інформаційних розрядів, l – кількість надлишкових розрядів для збільшення простору випадкових комбінацій.

З практичної точки зору збільшення довжини комбінацій $n \rightarrow \infty$ є неможливим, що зумовлює необхідність встановлення раціональних меж цього параметра. Суттєве збільшення n призводить до істотних обчислювальних і часових витрат, а також до зростання надлишковості, що знижує ефективність використання каналу. Крім того, навіть за умови статистичного шифрування залишається ймовірність витоку інформації через збереження певних закономірностей у шифрограмі. Це пояснюється тим, що внаслідок дії частотного аналізу можуть виявлятися статистичні зв'язки між окремими комбінаціями відкритого тексту та відповідними комбінаціями шифрограм. У результаті під час шифрування можуть зберігатися певні регулярності заміни символів. Для текстів будь-якої мови характерні такі статистичні особливості:

- повторюваність окремих букв і груп із двох або більше букв (m -грам);
- закономірності сполучуваності букв між собою;
- чергування голосних і приголосних, а також низка інших фонетико-графічних властивостей.

Усі ці особливості формують певний інформаційний «відбиток» мови, який частково може переноситися у шифрограму та використовуватися для криптоаналізу. Тому при проектуванні статистичного шифрування необхідно не лише прагнути до рівномірного розподілу комбінацій у просторі E_i , але й враховувати можливість маскування зазначених мовних закономірностей.

Як правило, існуючі статистичні характеристики текстів є досить стійкими, хоча й можуть мати певні відхилення, зумовлені тематикою чи жанровими особливостями повідомлення. Саме ця властивість стала основою одного з найефективніших методів криптоаналізу – частотного аналізу, який широко застосовується для розкриття системи шифрування. Суть цього методу полягає у дослідженні частоти появи окремих символів або їхніх комбінацій у зашифрованому тексті та порівнянні отриманих даних зі статистичними характеристиками відповідної мови.

Основна ідея частотного аналізу полягає в тому, що у більшості природних мов певні літери зустрічаються значно частіше за інші. Наприклад, в англійській мові найуживанішою є літера «е», а в українській – літера «о». Ця закономірність дозволяє криптоаналітику встановлювати ймовірні відповідності між символами відкритого тексту та шифрограми, поступово відновлюючи структуру повідомлення.

Таким чином, навіть при застосуванні статистичного шифрування повністю усунути ризики, пов'язані з частотними характеристиками, неможливо. Тому при побудові криптосистем доцільно враховувати не лише вимогу рівномірності комбінацій у шифрограмі, але й необхідність маскування частотних закономірностей, притаманних природним мовам.

Частотний аналіз ґрунтується на припущенні, що у зашифрованому тексті зберігаються характерні статистичні закономірності повідомлення, який

подається на шифратор, зокрема частотний розподіл символів. Для кожної мови існують власні частотні таблиці, які відображають ймовірність появи літер та їх комбінацій. Це дає можливість порівнювати частоти символів у шифрограмі з відомими статистичними даними певної мови.

Можна відзначити, що найбільш ефективно частотний аналіз застосовується до шифрів простої заміни (наприклад, шифр Цезаря або моноалфавітні шифри), у яких кожен символ відкритого тексту однозначно замінюється іншим символом. У таких випадках частотний розподіл літер зберігається, що дозволяє досить швидко встановити відповідність між літерами відкритого тексту і шифрограми.

Однак ефективність частотного аналізу значно знижується тоді, коли розподіл комбінацій у шифрограмі наближається до рівноймовірного. Крім того, аналіз може проводитися не лише для окремих літер, а й для біграм, триграм та довших послідовностей. Це дозволяє виявляти характерні словформи та стійкі мовні конструкції, які часто стають ключем для розкриття шифру.

Важливим чинником результативності частотного аналізу є обсяг наявної шифрограми. Чим більший обсяг тексту доступний криптоаналітику, тим точніше можна відновити статистичний розподіл символів та комбінацій. Натомість невеликі за обсягом шифрограми зазвичай не відображають типовий частотний профіль мови, що знижує ефективність методу.

Отже, частотний аналіз найбільш дієвий у випадках, коли шифрограма має значну довжину та не забезпечує вирівнювання розподілу символів [30, 56]. У такому разі ймовірність відновлення відповідностей між символами відкритого тексту та шифрограми істотно зростає.

З метою зменшення ефективності частотного аналізу у статистичному шифруванні застосовуються спеціальні методи маскування мовних закономірностей. Серед найбільш поширених підходів можна виділити:

1) періодичне введення додаткових псевдовипадкових символів у потік шифрограми, які не несуть інформаційного навантаження, але змінюють частотні характеристики повідомлення;

2) переставлення символів, яка полягає у зміні порядку слідування бітів або символів у кодовій матриці, що ускладнює відтворення первинної структури тексту та руйнує локальні закономірності;

3) застосування кодів зі змінною довжиною блоків, що потребує формування комбінацій різної довжини для представлення вихідних символів, що зменшує їх статистичні залежності;

4) адаптивне кодування, яке побудовано на том, що параметри кодування та переставлення вибираються залежно від частотних характеристик вхідного тексту, що дозволяє ефективніше маскувати закономірності конкретної мови.

5) комбінування з криптографічними примітивами, що припускає додаткове використання побітових операцій XOR, випадкових підстановок або генераторів псевдовипадкових чисел, які зменшують передбачуваність символів шифрограми.

Використання наведених методів забезпечує більш рівномірний розподіл символів у зашифрованому повідомленні та знижує ймовірність успішного застосування частотного аналізу. У результаті шифрограма наближається до випадкової послідовності, що значно підвищує її криптографічну стійкість. Для оцінки статистичних характеристик було проведено аналіз появи символів у текстах різного обсягу: $N_1 = 1424$; $N_2 = 3382$; $N_3 = 22336$. У табл. 4.3, 4.4 та 4.4 наведено результати дослідження, які демонструють, що відхилення ймовірності появи символів від середнього значення $p_j(c_j)$ залежить як від довжини тексту, так і від його тематики.

Наприклад, для літери «И» спостерігається поступове зменшення відхилень зі збільшенням обсягу тексту:

1) при $N_1 = 1424$ відхилення становить $\Delta_1(И) = 35,34\%$;

2) при $N_2 = 3382$ відхилення складає $\Delta_2(И) = 8,60\%$.

3) при $N_3 = 22336$ відхилення складає $\Delta_3(И) = 2,89\%$.

При цьому, простежується чітка статистична тенденція поступового наближення ймовірності появи літери «И» до середнього значення $p(И)=0,055$:

- 1) $p(И)_1=0,0744$ при $N_1=1424$;
- 2) $p(И)_2=0,060$ при $N_2=3382$;
- 3) $p(И)_3=0,0566$ при $N_3=22336$.

Разом з тим, для деяких символів виявлені аномальні відхилення, які не корелюють із зростанням обсягу тексту. Наприклад, для літери «У» отримані такі значення:

- 1) $p(У)_1=0,0295$ при $N_1=1424$;
- 2) $p(У)_2=0,0370$ при $N_2=3382$;
- 3) $p(У)_3=0,0373$ при $N_3=22336$.

При цьому відхилення від середньої ймовірності $p_j(У)=0,027$ складо:

- 1) $\Delta(У)_1=9,24\%$;
- 2) $\Delta(У)_2=37,99\%$;
- 3) $\Delta(У)_3=38,13\%$.

З отриманих результатів можна зробити висновок, що для літери «У» мінімальне відхилення ймовірності її появи спостерігається саме у тексті меншого розміру. Такі результати можуть вказувати на наявність певних статистичних аномалій, що не узгоджуються із загальною тенденцією наближення ймовірностей до середніх значень при збільшенні обсягу тексту.

Можна відзначити, що для літери «Ю» такі аномалії практично відсутні, про що свідчить статистика розподілу ймовірностей для різних довжин тексту:

- 1) $p(Ю)_1=0,0084$ при $N_1=1424$;
- 2) $p(Ю)_2=0,008$ при $N_2=3382$;
- 3) $p(Ю)_3=0,0079$ при $N_3=22336$.

У стовпчиках 4, 6 та 8 табл. 4.4 для текстів різної довжини ($N_1=1424$; $N_2=3382$; $N_3=22336$) наведено кількість простору випадкових комбінацій, що призначені для шифрування кожного символу, з урахуванням середньої ймовірності його появи у тексті. Розрахунок здійснюється за формулою:

$$N_i(c_j) = p_j(c_j) \times N_l, \quad (4.31)$$

де $p_j(c_j)$ – ймовірність появи символу c_j , N_l – загальна кількість символів у тексті.

Таблиця 4.3 – Відхилення ймовірності появи символів $p_j(c_j)$ від середнього значення $p_{j\text{сер}}(c_{j\text{сер}})$ в залежності від довжини та тематики тексту

Символ	Ймовірності $p_j(c_j), (p_{j\text{сер}}(c_{j\text{сер}}))$	Довжина тексту в символах N_l	Кількість комбінацій $N_i(c_j)$
И	0,0744 (0,055)	1424	199
И	0,0060 (0,055)	3382	186
И	0,0566 (0,055)	22336	1288
У	0,0295 (0,027)	1424	38
У	0,0370 (0,027)	3382	91
У	0,0373 (0,027)	22336	603
Ю	0,0084 (0,008)	1424	11
Ю	0,008 (0,008)	3382	27
Ю	0,0079 (0,008)	22336	176

У табл. 4.5 наведено приклади можливого розподілу випадкових комбінацій шифрування при кількості надлишкових біт $l = 1, 2, 3$ та за відомих значень ймовірностей появи символів у відкритому тексті. При цьому розмір алфавіту відкритого тексту вважається рівним $M_i=32$.

З теоретичної точки зору, використання для кожного символу власної множини випадкових кодових комбінацій різного обсягу $N_i(c_j)$, на виході статистичного шифратора забезпечує рівноймовірний їх розподіл. У такому випадку передбачається, що частково або повністю втрачається статистичний зв'язок між відкритим текстом та шифрограмою, що є важливою умовою підвищення криптостійкості. Однак реалізація такого підходу вимагає значних

обчислювальних ресурсів, що істотно ускладнює практичне застосування алгоритму. Тому доцільно розглянути спрощені варіанти розподілу випадкових комбінацій.

Спираючись на результати проведеного статистичного аналізу появи символів у текстах різного обсягу (табл. 4.6), запропоновано метод групування символів за близькими значеннями ймовірностей їхньої появи. Ідея полягає у тому, що ймовірності появи окремих символів можуть відхилятися від середніх значень $p_j(c_j)$ як у більшу, так і у сторону менших значень. Це дозволяє об'єднати символи з подібними характеристиками в групи та призначати їм спільні множини випадкових комбінацій, зменшуючи складність алгоритму без істотної втрати статистичної рівномірності.

У стовпчику 5 табл. 4.3 наведено приклад такого групування:

1) перша група має усього одну літеру «О», яка має середню ймовірність 0,086;

2) друга група – літери від «Н» до «И», де ймовірність появи змінюється від 0,055 до 0,068. Різниця між крайніми значеннями становить приблизно 0,013;

2) третя група – літери від «В» до «Е» з діапазоном ймовірностей від 0,042 до 0,046, що відповідає відношенню близько 1,09;

3) четверта група – літери від «С» та «К» з ймовірностями 0,037 та 0,033, де відмінність складає майже 1,12 рази;

4) п'ята група – літери від «М» до «П» (за початковими даними), з діапазоном від 0,025 до 0,029, де відношення між найбільшим і найменшим значенням становить 1,16.

Для прикладу, при надлишковості шифрування $l = 1$ довжина випадкових комбінацій дорівнює $k = m + l = 8 + 1 = 9$, де $m = 8$ – кількість бітів, необхідних для кодування символів алфавіту. Тоді загальна кількість можливих випадкових комбінацій визначається як:

$$N_l = 2^k. \quad (4.32)$$

Таблиця 4.4 – Статистичні показники появи символів залежно від розміру тексту

№	Символ	Середня імовірність $p_j(c_j)$ появи символі в тексті	Відхилення імовірності появи символів в текстах з різною довжиною від середньої імовірності					
			$N_1=1424$		$N_2=3382$		$N_3=22336$	
			1424	$\Delta(c_j)_1, \%$	3382	$\Delta(c_j)_2, \%$	22336	$\Delta(c_j)_3, \%$
1	О	0,086	0,0913	6,15	0,071	-17,48	0,0905	5,21
2	Н	0,068	0,0716	5,34	0,070	2,62	0,0582	-14,34
3	А	0,064	0,0765	19,60	0,101	58,01	0,0738	15,35
4	И	0,055	0,0744	35,34	0,060	8,60	0,0566	2,89
5	В	0,046	0,0456	-0,77	0,048	5,42	0,0532	15,63
6	Т	0,045	0,0597	32,65	0,050	11,05	0,0390	-13,44
7	І	0,044	0,0527	19,70	0,055	24,32	0,0520	18,13
8	Р	0,043	0,0456	6,15	0,055	27,90	0,0367	-14,62
9	Е	0,042	0,0428	1,99	0,057	35,87	0,0475	12,99
10	С	0,037	0,0449	21,47	0,034	-8,10	0,0374	1,16
11	К	0,033	0,0393	19,17	0,031	-6,82	0,0325	-1,37
12	М	0,029	0,0337	16,23	0,035	20,31	0,0313	7,91
13	У	0,027	0,0295	9,24	0,037	37,99	0,0373	38,13
14	Л	0,027	0,0449	66,46	0,048	78,50	0,0415	53,88
15	Д	0,027	0,0379	40,45	0,039	45,65	0,0282	4,30
16	П	0,025	0,0281	12,36	0,041	63,22	0,0263	5,12
17	З	0,020	0,0169	-15,73	0,025	22,71	0,0255	27,60
18	Я	0,019	0,0246	29,36	0,022	13,60	0,0336	76,96
19	Ь	0,016	0,0140	-12,22	0,013	-20,54	0,0103	-35,36
20	Б	0,013	0,0077	-40,58	0,011	-13,57	0,0172	32,25
21	Г	0,013	0,0147	13,44	0,013	0,08	0,0165	26,74
22	Ч	0,011	0,0133	21,30	0,007	-35,49	0,0138	25,77
23	Х	0,011	0,0140	27,68	0,009	-16,67	0,0084	-23,48
24	Ї	0,010	0,0000	-100,00	0,007	-34,95	0,0042	-58,36
25	Ц	0,010	0,0056	-43,82	0,008	-20,17	0,0077	-23,44
26	Й	0,009	0,0077	-14,17	0,008	-8,01	0,0124	38,29
27	Ю	0,008	0,0084	5,34	0,008	3,49	0,0079	-1,50
28	Ж	0,007	0,0049	-29,78	0,007	5,60	0,0075	6,81
29	Ш	0,005	0,0070	40,45	0,009	77,41	0,0088	75,50
30	Є	0,005	0,0042	-15,73	0,005	6,45	0,0035	-30,16
31	Щ	0,004	0,0042	5,34	0,002	-40,86	0,0077	91,40
32	Ф	0,003	0,0042	40,45	0,002	-31,01	0,0013	-56,72

Таблиця 4.5 – Використання чотирьох груп випадкових комбінацій для реалізації статистичного шифрування

№	Сим-вол	Середня ймовірність появи символів в тексті $p_j(c_j)$	Розподіл кількості випадкових комбінацій з урахування імовірності появи символів $p_j(c_j)$ в текстах з різною довжиною та загальної кількості випадкових кодових комбінацій $N_{\text{общ}}$					
			$l = 1$		$l = 2$		$l = 3$	
			$N_{l=1}=512, \gamma_{pe}=0,889$		$N_{l=2}=1024, \gamma_{pe}=0,8$		$N_{l=3}=2048, \gamma_{pe}=0,727$	
1	2	3	4	5	6	7	8	10
1	О	0,086	44	$N_{gr1}=44$ $N_1 = 44$	88	$N_{gr1}=88$ $N_1 = 88$	176	$N_{gr1}=88$ $N_1 = 88$
2	Н	0,068	35	$N_{gr2}=96$ $N_{2-4}=32$	70	$N_{gr2}=225$ $N_{2-4}=96$	139	$N_{gr2}=383$ $N_{2-4}=96$
3	А	0,064	33		66		131	
4	И	0,055	28		56		113	
5	В	0,046	24	$N_{gr3}=113$ $N_{5-10}=23$	47	$N_{gr3}=225$ $N_{5-10}=45$	94	$N_{gr3}=451$ $N_{5-10}=90$
6	Т	0,045	23		46		92	
7	І	0,044	23		45		90	
8	Р	0,043	22		44		88	
9	Е	0,042	22		43		86	
10	С	0,037	19	$N_{gr4}=36$ $N_{10-11}=18$	38	$N_{gr4}=72$ $N_{10-11}=36$	76	$N_{gr4}=143$ $N_{10-11}=72$
11	К	0,033	17		34		68	
12	М	0,029	15	$N_{gr5}=69$ $N_{12-16}=14$	30	$N_{gr5}=138$ $N_{12-16}=4$ 0	59	$N_{gr5}=276$ $N_{12-16}=80$
13	У	0,027	14		28		55	
14	Л	0,027	14		28		55	
15	Д	0,027	14		28		55	
16	П	0,025	13		26		51	
17	З	0,02	10	$N_{gr6}=20$ $N_{17-18}=10$	20	$N_{gr6}=40$ $N_{17-18}=20$	41	$N_{gr6}=80$ $N_{17-18}=40$
18	Я	0,019	10		19		39	
19	Ь	0,016	8	$N_{gr7}=33$ $N_{19-23}=7$	16	$N_{gr7}=66$ $N_{19-23}=13$	33	$N_{gr7}=131$ $N_{19-23}=26$
20	Б	0,013	7		13		27	
21	Г	0,013	7		13		27	
22	Ч	0,011	6		11		23	
23	Х	0,011	6		11		23	
24	Ї	0,010	5	$N_{gr8}=23$ $N_{24-28}=5$	10	$N_{gr8}=45$ $N_{24-28}=9$	20	$N_{gr8}=90$ $N_{24-28}=18$
25	Ц	0,010	5		10		20	
26	Й	0,009	5		9		18	
27	Ю	0,008	4		8		16	
28	Ж	0,007	4		7		14	
29	Ш	0,005	3	$N_{gr9}=9$ $N_{29-32}=2$	5	$N_{gr9}=17$ $N_{29-32}=4$	10	$N_{gr9}=35$ $N_{29-32}=9$
30	Є	0,005	3		5		10	
31	Щ	0,004	2		4		8	
32	Ф	0,003	2		3		6	

Розглянемо кодову швидкість статистичного шифрування при мінімальному значенні додаткового розряду $l = 1$. Кількість випадкових комбінацій становить при цьому становить $N_{l=1} = 512$, а кодова швидкість шифрування розраховується за формулою:

$$\gamma_{\text{ш}} = \frac{k}{n}. \quad (4.32)$$

де k – довжина кодової комбінації, n – загальна кількість бітів у шифрограмі.

Для $l = 1$ отримаємо $\gamma_{\text{ш}} = 0,889$. Вочевидь, що збільшення кількості надлишкових елементів l призводить до зменшення кодової швидкості $\gamma_{\text{ш}}$, проте одночасно забезпечує підвищення криптостійкості шифрування. Для $l = 2$ кількість випадкових комбінацій дорівнює:

$$N_{l=2} = 1024,$$

а для $l = 3$:

$$N_{l=3} = 2048.$$

У цих випадках кодова швидкість відповідно зменшується до $\gamma_{\text{ш}} = 0,8$ та $\gamma_{\text{ш}} = 0,787$, що відображає зниження частки корисної (конфіденційної) інформації в структурі шифрограми. Вочевидь, що зі збільшенням кількості груп статистичні характеристики вихідних даних шифратора в більший мірі стабілізуються, тобто розподіл випадкових комбінацій прагне до рівномірного закону.

При цьому кореляційних зв'язок вхідних символів, що поступають на шифратор, з вихідною послідовністю випадкових комбінацій мінімізується. Отже, вибір кількості груп об'єднання символів можна розглядати як інструмент адаптивного управління криптографічною стійкістю системи статистичного шифрування, яка також враховує ступінь складності перетворення даних.

Таблиця 4.6 – Статистичне шифрування з використанням дев'яти груп випадкових комбінацій

№	Сим-вол	Середня імовірність появи символі в тексті $p_j(c_j)$	Розподіл кількості випадкових комбінацій з урахування імовірності появи символів $p_j(c_j)$ в текстах з різною довжиною та загальної кількості випадкових кодових комбінацій $N_{\text{общ}}$					
			$l=1$		$l=2$		$l=3$	
			$N_{l=1}=512, \gamma_{pe}=0,889$		$N_{l=2}=1024, \gamma_{pe}=0,8$		$N_{l=3}=2048, \gamma_{pe}=0,727$	
1	2	3	4	5	6	7	8	10
1	О	0,086	44	$N_{gr1}=44$ $N_1=44$	88	$N_{gr1}=88$ $N_1=88$	176	$N_{gr1}=88$ $N_1=88$
2	Н	0,068	35	$N_{gr2}=96$ $N_{2-4}=32$	70	$N_{gr2}=225$ $N_{2-4}=96$	139	$N_{gr2}=383$ $N_{2-4}=96$
3	А	0,064	33		66		131	
4	И	0,055	28		56		113	
5	В	0,046	24	$N_{gr3}=113$ $N_{5-10}=23$	47	$N_{gr3}=225$ $N_{5-10}=45$	94	$N_{gr3}=451$ $N_{5-10}=90$
6	Т	0,045	23		46		92	
7	І	0,044	23		45		90	
8	Р	0,043	22		44		88	
9	Е	0,042	22		43		86	
10	С	0,037	19	$N_{gr4}=36$ $N_{10-11}=18$	38	$N_{gr4}=72$ $N_{10-11}=36$	76	$N_{gr4}=143$ $N_{10-11}=72$
11	К	0,033	17		34		68	
12	М	0,029	15	$N_{gr5}=69$ $N_{12-16}=14$	30	$N_{gr5}=138$ $N_{12-16}=40$	59	$N_{gr5}=276$ $N_{12-16}=80$
13	У	0,027	14		28		55	
14	Л	0,027	14		28		55	
15	Д	0,027	14		28		55	
16	П	0,025	13		26		51	
17	З	0,02	10	$N_{gr6}=20$ $N_{17-18}=10$	20	$N_{gr6}=40$ $N_{17-18}=20$	41	$N_{gr6}=80$ $N_{17-18}=40$
18	Я	0,019	10		19		39	
19	Ь	0,016	8	$N_{gr7}=33$ $N_{19-23}=7$	16	$N_{gr7}=66$ $N_{19-23}=13$	33	$N_{gr7}=131$ $N_{19-23}=26$
20	Б	0,013	7		13		27	
21	Г	0,013	7		13		27	
22	Ч	0,011	6		11		23	
23	Х	0,011	6		11		23	
24	Ї	0,010	5	$N_{gr8}=23$ $N_{24-28}=5$	10	$N_{gr8}=45$ $N_{24-28}=9$	20	$N_{gr8}=90$ $N_{24-28}=18$
25	Ц	0,010	5		10		20	
26	Й	0,009	5		9		18	
27	Ю	0,008	4		8		16	
28	Ж	0,007	4		7		14	
29	Ш	0,005	3	$N_{gr9}=9$ $N_{29-32}=2$	5	$N_{gr9}=17$ $N_{29-32}=4$	10	$N_{gr9}=35$ $N_{29-32}=9$
30	Є	0,005	3		5		10	
31	Щ	0,004	2		4		8	
32	Ф	0,003	2		3		6	

У табл. 4.4 наведено приклад варіанту розподілу випадкових комбінацій, де використано 15 груп. У кожену групу об'єднані символи з близькими значеннями середньої ймовірності їх появи. Такий підхід дозволяє більш точно врахувати статистичні властивості мови і забезпечити баланс між складністю та криптографічною стійкістю шифрування.

Додатково, зміна множин випадкових комбінацій для символів алфавіту в процесі статистичного шифрування ускладнює проведення криптоаналітичних атак. Це пов'язано з тим, що навіть при відомій частотній структурі мови противник не може напряду співвіднести символи відкритого тексту з комбінаціями у шифрограмі. У результаті загрози частотного аналізу значно знижуються.

4.8. Математичне моделювання криптографічної стійкості статистичного шифрування

Забезпечення високого рівня криптографічної стійкості [87-90] є ключовим завданням при побудові систем захисту інформації. Для статистичного шифрування важливим чинником, що визначає криптографічну стійкість алгоритму, є довжина випадкових кодових комбінацій, які розширюють простір можливих реалізацій та ускладнюють процедуру криптоаналізу. Саме за рахунок збільшення ентропії ключової послідовності підвищується рівень невизначеності для зловмисника та мінімізуються ймовірності успішного підбору ключа.

Математичне моделювання дозволяє оцінити залежність криптографічної стійкості від кількості додаткових біт, які перевищують довжину інформаційної комбінації для формування множини випадкових реалізацій статистичного шифрування. У даному підрозділі розглядаються відповідні формули для визначення методики підрахунку рівня криптографічної стійкості шифру залежно від довжини випадкової компоненти. Це забезпечує можливість

обґрунтувати вибір оптимальних параметрів статистичного шифрування для практичного застосування в ІКС.

У процесі статистичного шифрування кожна інформаційна комбінація представляється випадковою комбінацією довжиною $k = m + l$, яка вибирається з деякої множини реалізацій, закріпленої для кожного символу алфавіту. При цьому параметр l ($l = 1, 2, 3, \dots$) визначає кількість додаткових бітів для збільшення довжини випадкової комбінації k у порівнянні з інформаційною послідовністю m .

Таким чином, для кожної інформаційної комбінації замість єдиного коду існує множина можливих випадкових комбінацій, що збільшує простір варіантів з 2^m до 2^{m+l} . Це ускладнює задачу криптоаналізу, оскільки атакувальнику необхідно враховувати додаткову невизначеність, зумовлену параметром l .

Для повідомлення довжиною N_c символів обсяг невизначеності щодо рандомізації становить [45, 67, 68]:

$$H(R) = l \times N_c. \text{ (біт)} \quad (4.33)$$

Оцінка еквівалентного рівня безпеки, яка визначається мінімальною кількістю бітів, яку потрібно перебрати для зняття невизначеності задається наступною формулою:

$$S(l, N_c) = \min\{H(K) + lN_c, H(K) + H(M)\} \quad (4.34)$$

де $H(K)$ – ентропія ключа, $H(M)$ – ентропія повідомлення (верхня межа: $H(M) \leq mN_c$).

Отже, зростання параметра l призводить до збільшення простору випадкових комбінацій і, відповідно, до підвищення криптографічної стійкості системи статистичного шифрування.

З урахуванням даних табл. 4.4 визначимо ентропію джерела повідомлення:

$$H(M) = -\sum_{i=1}^{33} p_j(c_j) \log_2 p_j(c_j) = 4,7337.$$

Криптографічна стійкість для алгоритму з випадковими комбінаціями оцінюється за наступною формулою:

$$R_{\text{ст}} = H(K) - H(K|C) \quad (4.35)$$

де $H(K) = m + l$ – ентропія ключа, $H(K|C) = H(K) - H(M)$ – умовна ентропія.

Отже, для одного символу повідомлення можна відзначити криптографічну стійкість з урахуванням ентропії джерела:

$$R_{\text{ст сим}} = H(M) = 4,7337 \text{ біт.}$$

Для повідомлення з N_c символів отримуємо:

$$R_{\text{заг ст}} = N_c \times H(M) = N_c \times 4,7337.$$

За умови, що $l = 1$ визначимо ентропію ключа:

$$H(K) = \log_2 N_{l+1} = \log_2 512 = 9.$$

У цьому випадку умовна ентропія ключа $H(K|C)$ залежить від того, як розподілені випадкові комбінації. Розглянемо випадок, коли кількість випадкові комбінації розподіляються однакою для кожного символу алфавіту, тоді:

$$H(K|C) = H(K) - H(M) = 9 - 4,7337 = 4,2663.$$

Криптографічна стійкість на один символ для випадку $l = 1$ складає:

$$R_{\text{ст сим}} = H(K) - H(K|C) = H(M) = 4,7337 \text{ біт.}$$

Це означає, що стійкість на один символ не змінюється і залишається обмеженою ентропією джерела повідомлень.

В табл. 4.7 представлено криптографічна стійкість для повідомлення з $N_c = 10$ при різних значеннях l та рівномірному розподілу випадкових комбінацій статистичного шифрування.

Таблиця 4.7 – Криптографічна стійкість для повідомлення з $N_c = 10$ при різних значеннях l та рівномірному розподілу випадкових комбінацій статистичного шифрування

l	$H(K)$	$H(M)$	$R_{\text{ст сим}}$	$R_{\text{заг ст, біт}}$
1	9	4,7337	4,7337	47
2	10	4,7337	5,2663	53
3	11	4,7337	6,2663	63

При такому алгоритмі статистичного шифрування простежується кореляційний зв'язок між вхідними символами та шифрограмою, незважаючи на використання випадкових комбінацій. Це пояснюється нерівномірним характером розподілу ймовірностей символів повідомлення. При цьому кожен символ шифрується фіксованою кількістю випадкових комбінацій $N_{\text{вип}j} = N_{\text{вип}}/33$. Це створює статистичну залежність: шифрограми, що належать до підпростору частого символу (наприклад, "о"), будуть з'являтися частіше, ніж шифрограми для рідкісних символів.

З ростом значень l не усуває кореляцію між вхідними і вихідними потоками, а лише збільшує загальну кількість можливих шифрограм. Криптографічна стійкість на символ залишається обмеженою ентропією джерела $H(M)$, а не розміром ключа.

Для усунення цієї проблеми доцільним є перерозподіл випадкових комбінацій пропорційно з урахуванням середньої ймовірності появи символів в тексті. В цьому випадку умовна ентропія ключа втрачає $H(K|C) = 0$, тобто втрачається зв'язок між вхідними та вхідними комбінація, тоді:

$$R_{\text{ст сим пр}} = H(K). \quad (4.36)$$

В табл. 4.8 представлена криптографічна стійкість для повідомлення з $N_c = 10$ символів при різних значеннях l та пропорційному розподілу випадкових комбінацій для статистичного шифрування.

Таблиця 4.8 – Криптографічна стійкість для повідомлення з $N_c = 10$ при різних значеннях l та пропорційному розподілу випадкових комбінацій для статистичного шифрування

l	$H(K)$	$H(M)$	$R_{\text{ст сим}}$	$R_{\text{заг ст, біт}}$
1	9	4,7337	9	72
2	10	4,7337	10	100
3	11	4,7337	11	121
4	12	4,7337	12	133

Пропорційний розподіл випадкових комбінацій забезпечує вищу ентропію шифрограми на значення l один символ ($8 + l$ біт), що робить шифр стійкішим до статистичного аналізу. Бачимо, що в цьому випадку втрачаються статистичні властивості відкритого тексту випадковими комбінаціями, що підвищує криптографічну стійкість шифрограми.

4.9. Розробка методу інтеграції статистичного шифрування, завадостійкого кодування з декореляцією помилок

Розробка методу інтегрованого захисту інформації [44, 66, 67] на основі багатократного перетворення даних з використанням статистичного шифрування, завадостійкого кодування та декореляції помилок базується на необхідності забезпечити не лише криптографічну стійкість передаваної інформації, але й підвищити завадозахищеність каналу. Завадозахищеність включає показники завадостійкості та прихованості. Прихованість спрямована практично на всі рівня захисту інформації, яка передається в умовах РЕБ.

Водночас метод декореляції помилок [66] виконує критично важливу функцію по забезпеченню перетворення групових (пакетних) помилок, які виникають у каналі з завадами, у незалежні, рівномірно розподілених по кодовим блокам повідомлення. Завдяки декореляції є можливість більш ефективно використовувати коригувальні можливості кодів та суттєво зменшує ймовірність втрати інформації. При цьому, особливу увагу слід приділити властивостям коригувального коду. У класичному випадку, як правило, коригувальний код виконує лише функцію підвищення завадостійкості шляхом виявлення та виправлення помилок. Проте у запропонованому підході коригувальний код має виконувати подвійну роль: поєднувати функції завадостійкого кодування та додаткового шифрування. Це означає, що структура коду повинна забезпечувати не тільки корекцію помилок, а й ускладнювати відновлення вихідного повідомлення для злоумисника без знання ключа чи параметрів коду. Така інтеграція методів перетворення даних дозволяє сформулювати певні вимоги багаторівневого захисту інформації:

- 1) завадостійкість досягається за рахунок механізмів виявлення і виправлення помилок з додатковою функцією захисту інформації від НСД;
- 2) підвищення криптографічної стійкості обґрунтовується тим, що шифрограми, що отримані шляхом статистичного шифрування, прагнуть рівномірного закону розподілу;

3) декореляція помилок гарантує ефективне використання коригувальних можливостей та зменшує ризик компрометації даних, а також використовує додаткову функцію захисту інформації від НСД.

Таким чином, коригувальний код у системі інтегрованого захисту інформації має розглядатися не лише як інструмент завадостійкого кодування, але і як додатковий криптографічний механізм, що ускладнює реалізацію атак на систему. Це забезпечує комплексне підвищення стійкості до помилок і безпеки передавання інформації у заводових каналах.

Метод інтеграції статистичного шифрування, завадостійкого кодування та декореляції помилок розглянемо з урахуванням наступним чинників. Для ефективного використання пропускну здатності каналу необхідне його узгодження з джерелом інформації на вході. Згідно з основною теоремою Шеннона про кодування [65], ймовірність виникнення помилки під час передавання даних каналом із завадами наближається до нуля за умови, що довжина завадостійкого коду $n \rightarrow \infty$. У цьому випадку кодова швидкість визначається як [51]:

$$\gamma_k = \frac{k}{k+r} = \frac{k}{n} \rightarrow 1, \quad (4.37)$$

де k – кількість інформаційних біт, r – кількість перевірочних біт.

За умови (4.37) зростання r є незначним у порівнянні з обсягом інформаційної частини k . У табл. 4.9 наведено зміну показників γ_k для деяких показниках циклічного коду при збільшенні довжини кодового блоку та різних значеннях d_0 . Це свідчить про достатньо великі варіативні можливості по вибору коригувального коду для забезпечення необхідної завадостійкості з урахуванням статистичних особливостей розподілу помилок дискретного каналу.

Як зазначалося раніше, головним недоліком статистичного шифрування є його надлишковість, що впливає на швидкість передавання корисної інформації у каналі. Вочевидь, що зі збільшенням надлишкових елементів криптостійкість

системи статистичного шифрування підвищується, однак водночас зменшується кодова швидкість. Аналогічна закономірність спостерігаються і для завадостійкого кодування: як правило, зі зростанням надлишковості перевірочних елементів r підвищується його завадостійкість.

Розглянемо інтегрований підхід, за якого спочатку виконується статистичне шифрування, а потім застосовується завадостійке кодування. У такому випадку довжина кодового блоку визначається як:

$$n = k + l + r, \quad (4.38)$$

де l – додаткові біти, пов’язані зі статистичним шифруванням.

Таблиця 4.9 – Залежність γ_k від довжини кодового блоку циклічного коду та d_0

№	n	K	R	d_0	γ_k
1	31	19	12	4	0,612
2	33	23	10	3	0,696
3	33	13	10	5	0,393
4	63	45	18	7	0,714
5	63	51	12	4	0,809
6	127	106	21	7	0,834
7	127	114	13	4	0,897
8	255	231	24	7	0,905
9	255	242	13	4	0,949
10	511	484	27	7	0,947
11	511	497	14	4	0,972
12	1023	1009	14	4	0,986
13	2047	2002	15	4	0,978
14	4095	4080	15	4	0,996

При одночасному використанні статистичного шифрування та завадостійкого кодування ефективність системи можна оцінити за допомогою кодової швидкості, що розраховується за формулою [56]:

$$\gamma_{\text{шк}} = \frac{m}{m+l+r}. \quad (4.39)$$

Покажемо зв'язок використання пакетів різної довжини на ефективність системи зв'язку. Згідно з даними табл. 4.9, підвищити коефіцієнт $\gamma_{шк}$ можливо за рахунок збільшення довжини кодового блоку n . Відповідно до (4.37), доцільним є використання блоків більшої довжини. Проте в реальних системах передавання даних (ПД) зі зворотним зв'язком існують обмеження на максимальну довжину пакета. Це пояснюється тим, що з ростом довжини пакета зростає і вплив випадкових завад, що, у свою чергу, призводить до збільшення кількості повторних запитів.

Ефективна швидкість системи ПД зі зворотним зв'язком оцінюється за допомогою коефіцієнтів γ_k і γ_e [51] і визначається як:

$$R_e = \gamma_k \cdot \gamma_e = \frac{1 - P_{ст}(n)}{1 + (M - 1) \cdot P_{ст}(n)}, \quad (4.40)$$

де M – кількість повторних передач кодових блоків, γ_e – коефіцієнт, що враховує ймовірність повторних запитів пакета, $P_{ст}$ – ймовірність стирання пакета.

Розглянемо умову вибору оптимальної довжини пакету. При збільшенні довжини пакета n підвищується ймовірність його спотворення. Це призводить до того, що $\gamma_k \rightarrow 1$, $\gamma_e \rightarrow 0$, а відповідно й ефективна швидкість системи передавання $R_e \rightarrow 0$. На рис. 4.4 наведені залежності відповідних коефіцієнтів від довжини пакета, з яких можна зробити висновок про умову вибору оптимальної довжини пакету $n_{опт}$ [56]:

$$\gamma_k = \gamma_e. \quad (4.41)$$

Бачимо, що в цьому випадку досягається максимальне значення ефективної швидкості за умови:

$$R_e = R_{max}. \quad (4.42)$$

Отже, при інтеграції статистичного шифрування та завадостійкого кодування виникає компроміс: збільшення довжини кодового блоку дозволяє підвищити коефіцієнт $\gamma_{\text{шк}}$ та більш ефективно використовувати пропускну спроможність каналу, проте водночас робить систему більш вразливою до випадкових завад і збільшує кількість перезапитів. Тому вибір оптимальної довжини пакета має здійснюватися з урахуванням як криптостійкості, так і завадостійкості, а також реальних умов функціонування системи передавання даних.

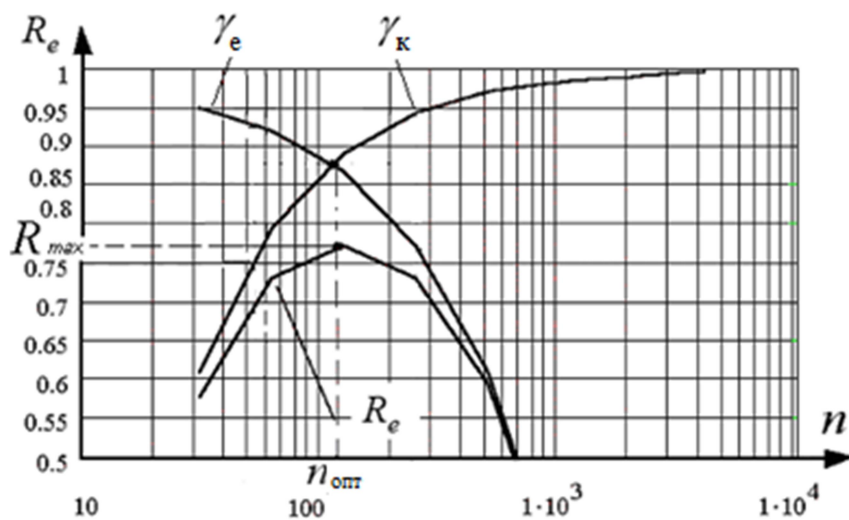


Рисунок 4.4 – Залежність R_e , γ_k і γ_e від довжини пакету n

Розглянемо інтеграцію статистичного шифрування та завадостійкого кодування на основі ітеративного коду, у якому контрольні елементи формуються бітами перевірки на парність. Запропонований ітеративний код має виконувати подвійну функцію: по-перше, забезпечувати завадостійкість шляхом виявлення/виправлення помилок у процесі багаторазового перерахунку паритетів; по-друге, реалізовувати шифрувальну складову за рахунок несистематичного розміщення контрольних бітів і ключ-керованого перемішування даних та перевірочних елементів. Такий підхід дозволяє одночасно підвищити ймовірність коректного приймання та ускладнити відновлення первинного повідомлення без знання параметрів коду й секретних перестановок.

Алгоритм побудови такого ітеративного коду базується на формуванні перевірконої матриці H , у якій кожне кодове слово подається у вигляді вектору, що включає як випадкові комбінації статистичного шифрування, так і перевірочні біти. Для завадостійкого кодування використовується двовимірна перевірна матриця виду

$$H = n \times v, \quad (4.43)$$

де $n = t + l + r$ – загальна кількість біт у рядку, v – кількість комбінацій у матриці.

Структура H -матриці має наступний вигляд:

$$H = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1j} & p_{1m} \\ x_{21} & x_{22} & \dots & x_{2j} & p_{2m} \\ \vdots & \vdots & & \vdots & \vdots \\ x_{g1} & x_{gv} & \dots & x_{gj} & p_{gm} \\ p_{v1} & p_{v2} & \dots & p_{vj} & p_{vm} \end{bmatrix} \quad (4.44)$$

де $x_{11}, x_{12}, \dots, x_{1j}$ – випадкові комбінації, сформовані в результаті статистичного шифрування, $p_{1m}, p_{2m}, \dots, p_{gm}, p_{vm}$ – перевірочні елементи рядків, $p_{v1}, p_{v2}, \dots, p_{vj}$ – перевірочні елементи стовбців.

Згідно з класичним визначенням, код може виправляти:

$$t_{\text{вип}} = \frac{d_0 - 1}{2}, \quad (4.45)$$

для непарного значення d_0 , або

$$t_{\text{вип}} = \frac{d_0 - 2}{2}, \quad (4.46)$$

для парного значення d_0 .

Це означає, що звичайний код з одним бітом парності не виправляє помилки, а лише їх виявляє, тобто $t_{\text{вия}} = 1$ (4.45) та $t_{\text{вип}} = 0$ (4.46).

Для ітеративного коду з рядками і стовпцями, в якому використовується двовимірна перевірка на парність забезпечується наступна загальна мінімальна кодова відстань [50]:

$$d_{0\text{заг}} = d_0 \times d_0. \quad (4.47)$$

В цьому випадку для даного ітеративного коду отримаємо наступні кратності виявлення $t_{\text{вия}} = 3$ (4.45) та виправлення $t_{\text{вип}} = 1$ (4.46). Перевірочні біти для рядків p_{gm} та стовпчиків формуються за правилом парності:

$$p = \bigoplus_i^j x_i, \quad (4.48)$$

де $\bigoplus$ – операція XOR, x_i – біти рядків або стовпчиків.

Коригувальна здатність ітеративного коду полягає в наступному. Якщо під час передачі відбулася одинична помилка, то невідповідність між контрольними бітами рядків і стовпчиків дозволяє точно визначити її позицію та виправити. Якщо виникають подвійні помилки в одному рядку, то вони виявляються, але виправити їх неможливо. У випадку більшої кількості помилок можливе лише часткове виявлення залежно від структури коду.

Отже, можна відзначити, що біти парності виконують подвійну роль: забезпечують певний рівень завадостійкості у каналі зв'язку; одночасно підтримують функцію шифрування, оскільки перевірочні біти беруть участь у формуванні шифрограми.

Для подальшого підвищення криптостійкості статистичного шифрування за допомогою ітеративного коду введемо для нього додаткову функцію шифрування, яка інтегрується у структуру матриці H . Розглянемо наступні варіанти додаткових механізмів шифрування:

1) Перестановка бітів, яке виконується після формування рядків і стовпчиків матриці з використанням псевдовипадкового перемішування елементів. Для виконання цього перетворення використовується ключ, до допомогою якого шляхом генерації псевдовипадкових чисел формується матриця перестановок. Це унеможливило б прямий аналіз структури перевірочних бітів;

2) Використання для інформаційних та перевірочних бітів процедури XOR з бітами ключової послідовності, згенерованої генератором псевдовипадкових чисел;

3) Реалізація адаптивної надлишковості, яка полягає у зміні кількості перевірочних бітів у рядках і стовпчиках залежно від статистичних властивостей вхідного повідомлення, що також сприяє ускладненню криптоаналізу перехопленої шифрограми. Криптографічна стійкість у такій схемі визначається за допомогою наступних параметрів:

- 1) довжиною інформаційного блоку $m + l$;
- 2) кількістю надлишкових бітів l статистичного шифрування;
- 3) кількістю перевірочних бітів r ;
- 4) параметрами перестановки або генератора ключової послідовності.

Отже, матриця H одночасно виконує функції контролю помилок та шифрування: вона містить випадкові комбінації даних, а також систему перевірочних бітів, що забезпечує виявлення й виправлення спотворень в приймачі. Розглянемо завадостійкий ітеративний код з функцією шифрування.

При кодуванні ітеративним кодом до кожної випадкової комбінації додаються контрольні біти, які визначаються на основі перевірок парності. Для кожного рядка матриці перевірки H обчислюється рівняння парності, що охоплює певну підмножину інформаційних бітів:

$$\begin{aligned}
p_{1m} &= x_{11} \oplus x_{12} \oplus \dots \oplus x_{1j} \\
p_{2m} &= x_{21} \oplus x_{22} \oplus \dots \oplus x_{2j} \\
&\dots \\
p_{gm} &= x_{g1} \oplus x_{g2} \oplus \dots \oplus x_{gj} \\
p_{vm} &= x_{v1} \oplus x_{v2} \oplus \dots \oplus x_{vj}
\end{aligned}
\tag{4.49}$$

Кожне таке рівняння парності відповідає одному рядку матриці H і забезпечує контроль цілісності відповідної групи бітів випадкової комбінації. Аналогічно обчислюються контрольні біти $p_{v1}, p_{v2}, \dots, p_{vj}$ для стовпчиків матриці. Таким чином, сформоване кодове слово має структуру:

$$x_{11}x_{12} \dots x_{1j}p_{1m}x_{21}x_{22} \dots x_{2j}p_{2m} \dots x_{g1}x_{gv} \dots x_{gj}p_{gm}p_{v1}p_{v2} \dots p_{vj}p_{vm}.$$

Отже, додавання перевірочних бітів забезпечує можливість виявлення та часткового виправлення помилок, що виникають під час передавання, підвищуючи надійність і стійкість статистичного шифрування.

Для підвищення криптографічної стійкості доцільним є використання змінної структури матриці перевірок H . Це означає, що в одному рядку такої матриці можуть одночасно міститися біти з різних випадкових комбінацій. Завдяки цьому досягається перехресне зв'язування інформаційних і перевірочних елементів, що ускладнює статистичний аналіз та зменшує ймовірність успішного відновлення вихідних даних противником.

Вкраплення перевірочних елементів у кодове слово, а також зміна розміру матриці H додатково підвищує структурну прихованість кодових комбінацій. Якщо ж параметри матриці H періодично змінювати, то це створює динамічний захисний ефект, який значно ускладнює проведення атак на шифрограми статистичного шифрування, адже простір можливих варіантів для аналізу зростає експоненційно.

З точки зору корегувальних властивостей, ітеративний код із перевіркою на парність характеризується мінімальною кодовою відстанню між дозволеними комбінаціями $d_{0iter} = 4$. Це означає, що код здатний виявляти

помилки кратності $t_{\text{вияв}} = d_{0\text{ітер}} - 1 = 3$, а також виправляти помилки з кратністю $t_{\text{випр}} = 1$. Отже, даний код може: виправляти однократні помилки; виявляти до трьох одночасних помилок; фіксувати помилки за допомогою синдромів, обчислених як по рядках, так і по стовпчиках матриці. В табл. 4.10 надано аналіз впливу параметрів ітеративного коду на криптографічну стійкість та коригувальну здатність коду.

Таблиця 4.10 – Вплив параметрів ітеративного коду на криптографічну стійкість та коригувальну здатність коду

Модифікація ітеративного коду	Вплив на криптографічну стійкість	Вплив на виявлення та виправлення помилок
Зміна розміру матриці H	Ускладнює статистичний аналіз; зростає простір можливих кодових комбінацій за рахунок перевірочних елементів	Можливість збільшення кількості перевірочних бітів для підвищення коригувальної здатності коду
Вкраплення перевірочних елементів у кодове слово	Підвищує структурну прихованість та ускладнює криптоаналіз	Забезпечує додаткові контрольні суми для локалізації помилок
Періодична зміна параметрів матриці H	Створює динамічність структури коду, зменшує ризик атак на основі аналізу повторів	Не впливає безпосередньо на корекцію, але ускладнює прогнозування синдрому помилок противником
Зміна мінімальної кодової відстані $d_0 \geq 4$	Опосередковано підсилює стійкість до атак, оскільки помилки складніше використати для статистичного відновлення	Дає можливість виправляти 1 помилку і виявляти до 3-х одночасних помилок
Адаптивна зміна параметрів матриці в часі	Підвищує захист від довготривалих атак та статистичного моделювання	Забезпечує задану завадостійкість при зміні умов передавання сигналу

Ітеративні коди з перевіркою на парність забезпечують не лише завадостійкість, але й додаткову криптографічну стійкість у системах статистичного шифрування. Зміна розміру матриці H , динамічне вкраплення перевірочних бітів та періодична модифікація параметрів коду ускладнюють аналіз шифрограм і знижують ефективність атак на основі статистичного відновлення. При цьому мінімальна кодова відстань $d_0 = 4$ дозволяє виявляти до трьох помилок та виправляти одну, що забезпечує базовий рівень захисту від

завад. У поєднанні ці властивості створюють гнучкий механізм, який одночасно підвищує і стійкість до атак, і надійність передачі інформації.

Розглянемо наступний рівень інтеграції статистичного шифрування та завадостійкого кодування із застосуванням механізму декореляції помилок. Традиційно декореляція використовувалася переважно для підвищення ефективності виправлення помилок у системах зв'язку, проте в задачах захисту інформації від НСД її можливості не були достатньо розкриті.

Основна ідея декореляції полягає у зменшенні ймовірності виникнення групових помилок, що формуються внаслідок імпульсних або завадових впливів у каналі передавання. Для цього здійснюється перестановка бітів кодових блоків таким чином, щоб біти одного й того ж блоку не передавалися послідовно, а розносилися на певну відстань у передавальному потоці.

Завдяки такій обробці навіть у разі впливу імпульсної завади помилки не концентруються у межах одного кодового блока, а розподіляються між різними блоками. Це запобігає утворенню багатократних помилок, які виходять за межі корегувальної здатності завадостійкого коду. Таким чином, без збільшення надлишковості коду забезпечується більш ефективне виправлення помилок.

У приймальній частині після декодування виконується операція зворотної перестановки, що дозволяє відновити початковий порядок бітів. При цьому розподіл помилок між різними комбінаціями повідомлення знижує кратність помилок у кодових блоках і підвищує ефективність їх виправлення.

На рис. 4.5 подано принцип дії механізму декореляції помилок із збереженням внутрішньої структури кодових блоків. Бачимо, що базовий метод декореляції помилок передбачає найпростіший перерозподіл бітів між кодовими блоками з метою зниження ймовірності групових помилок. Проте такий підхід не враховує можливості одночасного підвищення криптографічної стійкості.

Для досягнення подвійного ефекту – захисту від завад та посилення криптографічної стійкості – доцільно перед етапом декореляції застосовувати внутрішньоблокову перестановку бітів за певними правилами $\Pi_1, \Pi_2 \dots \Pi_N$. Такі

правила визначають порядок переміщення бітів усередині кожного кодового блока і можуть змінюватися динамічно, наприклад, залежно від ключа або генератора псевдовипадкових послідовностей). Після виконання внутрішньоблокової перестановки здійснюється стандартна операція декореляції – рознесення бітів між різними блоками (рис. 4.6). Таким чином формується подвійна операція:

- 1) внутрішньоблокове шифрування шляхом перестановки бітів за правилами $\Pi_1, \Pi_2 \dots \Pi_N$;
- 2) міжблокова декореляція для зниження ймовірності групових помилок у каналі.

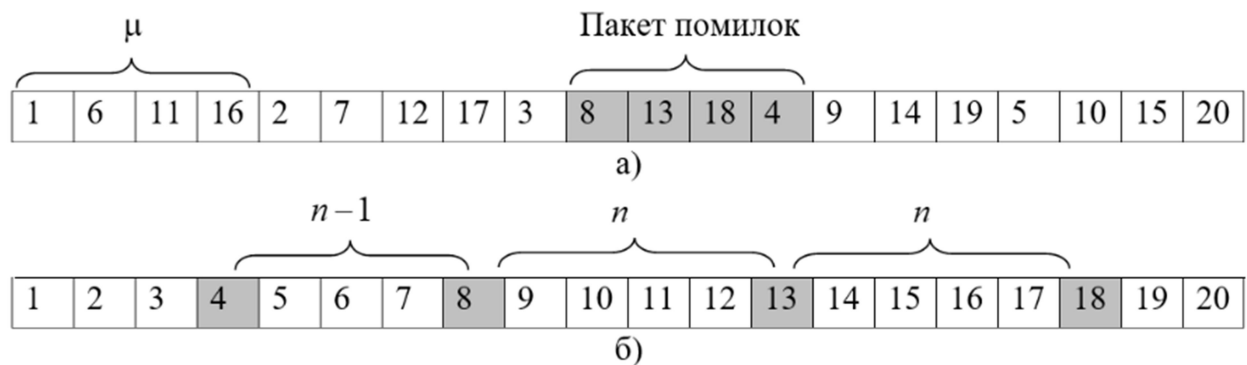


Рисунок 4.5 – Декореляції помилок із збереженням порядку розташування елементів у кодових блоках

У результаті формується механізм, який можна визначити як декореляцію помилок із вбудованою функцією шифрування. Такий підхід одночасно:

- 1) ускладнює криптоаналіз, оскільки порядок бітів у межах блоків змінюється за ключовими правилами;
- 2) знижує ефективність атак на основі аналізу кореляцій між бітами;
- 3) забезпечує стійкість до імпульсних завад без збільшення надлишковості завадостійкого коду.

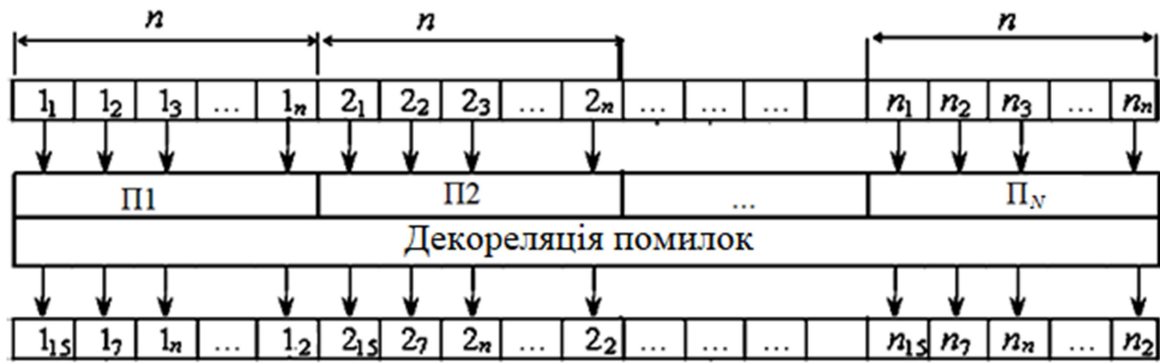


Рисунок 4.6 – Метод декореляції помилок з функцією шифрування

Отже, інтеграцію статистичного шифрування, завадостійкого кодування та декореляції помилок доцільно розглядати як трирівневу систему захисту інформації від НСД та випадкових завад у каналі. Кожен рівень цієї системи використовує власний механізм введення надлишковості та вирішує специфічні завдання щодо захисту інформації:

1) Перший рівень – статистичне шифрування. Забезпечує захист від НСД шляхом генерації випадкових комбінацій довжиною $m + l$. Для цього потрібне використання додаткових біт l , кількість яких безпосередньо визначає криптографічну стійкість методу.

2) Другий рівень – завадостійке кодування на основі ітеративного або іншого коду. Забезпечує захист від випадкових завад, а також завдяки вкрапленню перевірочних біт у структуру випадкових кодових блоків підвищує криптостійкість методу статистичного шифрування.

3) Третій рівень – декореляція помилок. Сприяє підвищенню завадостійкості завдяки зменшенню групування помилок у кодових блоках. Додатково цей рівень забезпечує підвищення криптографічної стійкості за рахунок перестановки біт у межах кодових блоків відповідно до певних правил $\Pi_1, \Pi_2 \dots \Pi_N$.

Характеристики рівнів інтегрованого захисту інформації від НСД та випадкових завад наведені у табл. 4.11. Процес перетворення даних для такої системи захисту інформації представлено на рис. 4.11.

Узагальнена структурна схема перетворення даних на основі інтеграції статистичного шифрування, завадостійкого кодування та декореляції помилок представлена на рис. 4.7. Ця схема характеризується за наступними параметрами:

- 1) k – кількість біт у рядку після статистичного шифрування;
- 2) s – кількість кодових блоків у матриці;
- 3) $r_{\text{заг}} = r_{\text{ряд}} + r_{\text{ст}}$ – загальна кількість перевірочних біт у рядках та стовпцях ітеративного коду;
- 4) $k_{\text{заг}} = m \times s$ – загальна кількість інформаційних біт, що беруть участь у процесі завадостійкого кодування;;
- 5) $n_{\text{заг}} = s(m + l) + r_{\text{заг}}$ – загальна кількість біт в ітеративному коді;
- 6) $r_{\text{ряд}}, r_{\text{ст}}$ – кількість перевірочних біт для кожного рядка та стовпця;
- 7) r_{Σ} – загальна кількість перевірочних елементів.

Таблиця 4.11 – Характеристики рівнів інтегрованого захисту інформації

№	Ступені захисту інформації	Склад кодового блоку		
		Кількість біт у комбінації	Додаткові біти	Вид захисту
1	Статистичне шифрування	m	l	Захист від НСД
2	Завадостійке кодування випадкових комбінацій на основі ітеративного або іншого коду з функцією шифрування	$m + l$	r	Забезпечується завадостійкість та підвищується криптостійкість кодових блоків
3	Декореляція помилок з функцією шифрування	$m + l + r$	Не потрібні	Сприяє підвищенню завадостійкості та криптостійкості

На рис. 4.8 наведено структурну схему статистичного шифрування з інтеграцією завадостійкого кодування та декореляцією помилок, у якій параметри перетворення даних можуть змінюватися відповідно до заданого алгоритмі на кожній ступені захисту інформації.

Джерело інформації (ДІ) формує послідовність символів b_i , які подаються на пристрій кодування (ПК) і перетворюються у кодові комбінації довжиною m . Далі кожна комбінація обробляється блоком випадкових комбінацій (БВК), у результаті чого формується випадкова комбінація довжиною $k = m + l$.

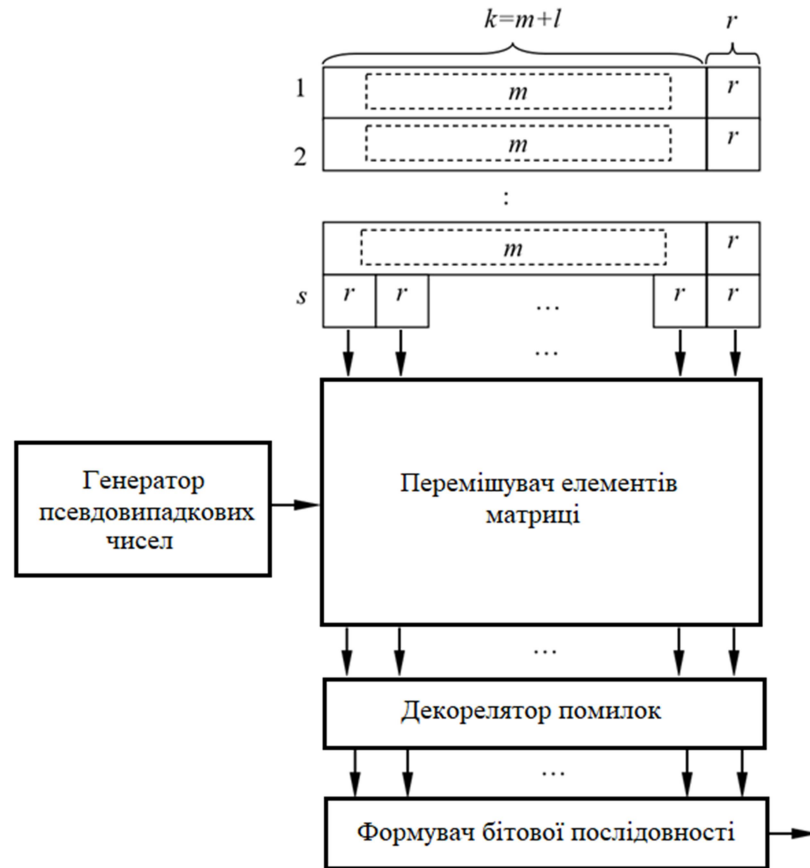


Рисунок 4.7 – Процес перетворення даних для трирівневої системи захисту інформації

Ймовірнісний аналізатор (ІА) оцінює розподіл імовірностей $p_j(u_i)$ символів b_i з алфавіту повідомлення. На основі отриманих значень та кодової книги (КГ1) визначається кількість випадкових кодових комбінацій для кожного символу. Загальна кількість можливих випадкових комбінацій $N_{\text{заг}} = 2^k$ залежить від обраного параметра l . Для кожної інформаційної комбінації Q_i за допомогою генератора випадкових чисел (ГВЧ) обирається випадкова реалізація $c_j \in C$, що забезпечує процес статистичного шифрування.

На наступному етапі пристрій завадостійкого кодування (ПЗК) формує ітеративну матрицю з урахуванням параметрів від кодової книги (КГ2),

поточний стан якої визначається генератором псевдовипадкових чисел (ГПВЧ-1). У структуру випадкових комбінацій вбудовуються перевірочні біти рядків і стовпчиків для завдання забезпечення певного рівня завадостійкості і криптостійкості. Розмірність матриці може змінюватися відповідно до параметрів КГ2.

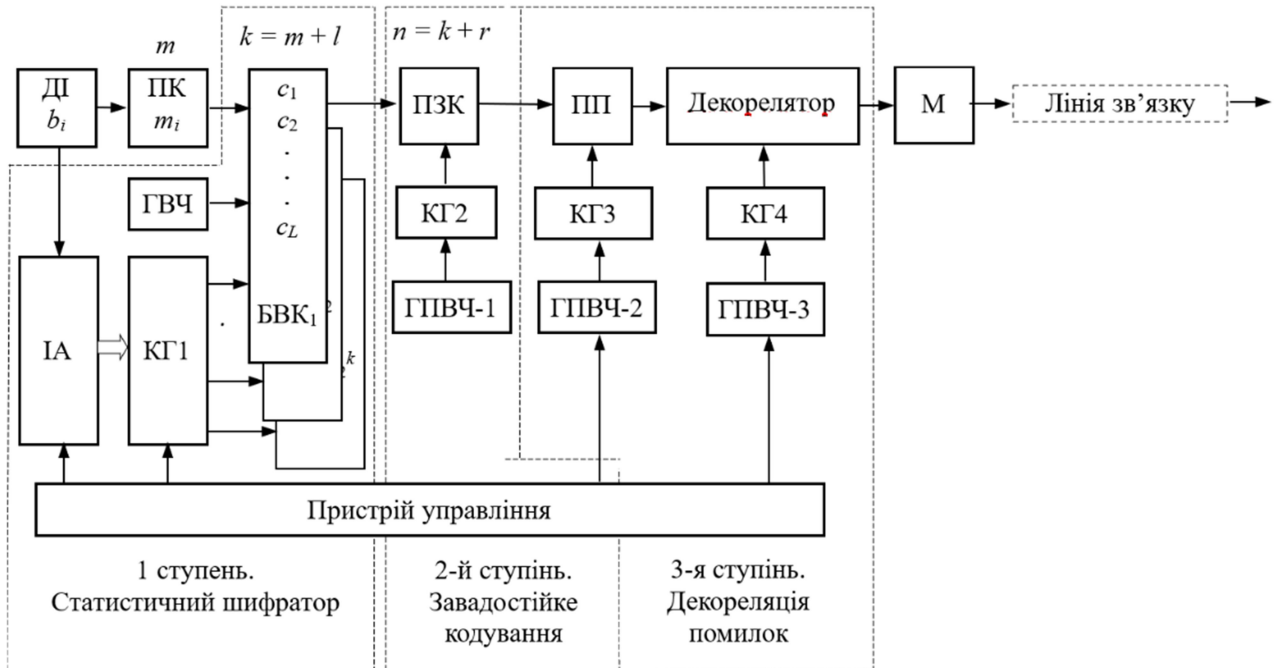


Рисунок 4.8 – Структурна схема системи статистичного шифрування з інтеграцією завадостійкого кодування з декореляцією помилок

Пристрій перестановки (ПП) виконує перемішування бітів у межах кодових блоків за певними правилами, що задаються кодовою книгою (КГ3). Поточний стан КГ3 визначається генератором псевдовипадкових чисел (ГПВЧ-2). Це забезпечує додаткове ускладнення структури кодових слів.

Заключний етап – пристрій декореляції, у якому відбувається часовий рознос бітів кодових блоків для зменшення ймовірності виникнення групових помилок у каналі. Параметри декореляції також задаються КГ3, що керується ГПВЧ-3. У результаті забезпечується стійкість системи як до випадкових завад, так і до спроб несанкціонованого доступу.

4.10. Компенсація надлишковості комбінованих методів захисту інформації за допомогою таймерних сигналів

Результати дослідження таймерних сигналів підтвердили можливість підвищення структурної прихованості та одночасної компенсації надлишковості випадкових комбінацій статистичного шифрування і перевірочних елементів завадостійкого коду [92-94]. Важливою перевагою таймерного кодування є також можливість реалізації завадостійкого кодування. З цією метою для контролю вірності передавання доцільно використовувати дозволені таймерні сигнали із визначеною мінімальною кодовою відстанню d_0 .

Наприклад, для $d_{0\text{ТСК}} = 4$, $n = 7$, $i = 3$, $s = 5$, згідно з виразом (3.26), із загального числа реалізацій $N_{p\text{ТСК}} = 1771$ можна отримати методом перебору $N_{\text{доз ТСК}} = 146$ дозволених конструкцій (табл. 3.5), тоді як при використанні рівняння якості (3.30) при $A_0=19$, $A_1=2$, $A_2=3$, $A_3=7$ можна отримати усього $N_{\text{доз ТСК}} = 93$. Зі збільшенням значення $d_{0\text{ТСК}}$ кількість дозволених комбінацій зменшується. Так, при $d_{0\text{ТСК}} = 5$ кількість дозволених комбінацій при повному переборі вона становить $N_{\text{доз ТСК}} = 79$ (табл. 3.5), а при використанні рівняння якості усього $N_{\text{доз ТСК}} = 37$.

Таким чином, особливості формування дозволених ТСК необхідно враховувати під час розроблення методів підвищення структурної прихованості передавання та забезпечення необхідної достовірності інформації. У табл. 3.6 для рівняння якості (3.30) наведено значення коефіцієнтів A_0 , A_1 , A_2 і A_3 , за яких можливе формування реалізацій ТСК із різними значеннями $d_{0\text{ТСК}}$.

Як бачимо з табл. 4.13, використання на етапі таймерного кодування комбінації двох ТСК, одна з яких є дозволеною, дозволяє суттєво збільшити кількість реалізацій для передавання комбінацій РЦК. Наявність хоча б однієї дозволеної ТСК гарантує збереження мінімальної кодової відстані $d_{0\text{ТСК}}$.

Подвоєння інтервалу передавання ТСК ($m_{\text{ТСК}12}=2m_{\text{ТСК}}$) забезпечує компенсацію надлишковості стохастичного шифрування та завадостійкого кодування. Якщо врахувати, що двійковий код із довжиною $n_{\text{рцк}}=21$ біт

замінюється на ТСК із $m_{\text{ТСК}12} = 14$ елементів, тоді кодова швидкість зростає у 1,5 разів.

Таблиця 4.12 – Кількість дозволених ТСК в залежності від n, s, i, d_0 и $A_0=19, A_1=2, A_2=3, A_3=7$ при використанні двох ТСК

№	Параметри ТСК			Загальна кількість реалізацій	Вибірki дозволених комбінацій при використанні двох ТСК в залежності від d_0					
	n	i	s		4	5	6	7	8	9
1	7	3	5	1771	65527	47817	42504	26565	23023	65527
2	7	3	6	2925	172575	125775	119925	67275	55575	172575
3	7	3	7	4495	395560	305660	260710	152830	130355	395560
4	8	3	5	3276	212940	170352	131040	88452	72072	212940
5	8	3	6	5456	578336	447392	371008	229152	190960	578336
6	8	3	7	8436	1316016	1037628	826728	506160	413364	1316016

Таблиця 4.13 – Кількість дозволених комбінацій в залежності від n, s, i, d_0 і $A_0=19, A_1=2, A_2=3, A_3=7$ при використанні двох ТСК

№	Параметри ТСК			Загальна кількість реалізацій	Вибірki дозволених комбінацій при використанні двох ТСК в залежності від d_0		
	n	i	s		4	5	6
1	7	3	5	1771	65527	47817	42504
2	7	3	6	2925	172575	125775	119925
3	7	3	7	4495	395560	305660	260710
4	8	3	5	3276	212940	170352	131040
5	8	3	6	5456	578336	447392	371008
6	8	3	7	8436	1316016	1037628	826728

Вочевидь, що можливе застосування множин ТСК з більшим значенням параметра s , однак у цьому випадку рівень завадостійкості знижується, що необхідно враховувати при виборі параметрів побудови сигнальних конструкцій.

Висновки

1. Обґрунтовано необхідність комбінованого застосування криптографічних та завадостійких методів, що забезпечує комплексний захист

інформації не лише від НСД, але й від впливу випадкових завад у каналі зв'язку.

2. Запропоновано багаторівневу структуру захисту, яка включає статистичне шифрування, завадостійке кодування та декореляцію помилок. Кожен рівень виконує окремі функції, а їх інтеграція дозволяє досягти синергетичного ефекту.

3. Доведено взаємозв'язок між параметрами перетворень (кількість додаткових біт, розмірність кодових блоків, мінімальна кодова відстань) та критеріями захищеності: криптографічною стійкістю та достовірністю.

4. Розроблено методи формування шифрограм із варіативними комбінаціями та простору випадкових кодових слів з урахуванням статистики алфавіту та ймовірностей появи символів. Це дозволило підвищити ентропію шифрограм та ускладнити криптографічний аналіз шифрограм.

5. Побудовано математичні моделі криптографічної стійкості статистичного шифрування, які показали ефективність використання пропорційного розподілу випадкових комбінацій порівняно з рівномірним.

6. Запропоновано інтеграцію процесів статистичного шифрування і завадостійкого кодування з декореляцією помилок, в яких додатково вбудовані механізми захисту від НСД, що забезпечує підвищення загальної криптографічної стійкості та захист від групових помилок у каналі без значного збільшення надлишковості перевірочних елементів.

7. Доведено, що використання таймерних сигналів дозволяє компенсувати надлишковість комбінованих методів захисту інформації, підвищити структурну прихованість шифрограм і забезпечити додаткову завадостійкість системи передачі.

5 ДОСЛІДЖЕННЯ ТА ОБҐРУНТУВАННЯ ВИБОРУ ПАРАМЕТРІВ ТАЙМЕРНИХ СИГНАЛІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА

У розділі здійснено аналіз параметрів таймерних сигналів для завдання формування шумоподібних сигналів у системах захисту інформації. Обґрунтовано критерії вибору параметрів ТСК з урахуванням вимог до завадостійкості, прихованості та складності реалізації сигнальних конструкцій. Показано, що здатність таймерного кодування генерувати велику кількість варіантів реалізацій, залежно від параметрів їх побудови, дозволяє підвищити рівень структурної прихованості.

Проаналізовано вплив кожного з параметрів на ключові характеристики сигналу, включаючи обчислювальну складність, надійність передачі та рівень інформаційної маскуваності. Визначено обмеження та оптимальні діапазони значень параметрів, які забезпечують ефективне функціонування шумоподібних таймерних сигналів при використанні методів розширення спектра.

Результати розділу формують теоретичну та практичну базу для побудови завадозахищених та прихованих каналів зв'язку на основі ТСК з адаптованими параметрами.

5.1. Основні завдання при побудові шумоподібних сигналів на основі таймерного кодування

При вирішенні завдання використання ТСК для синтезу шумоподібних сигналів [21, 58, 76] важливим є обґрунтований вибір параметрів побудови ТСК. Доцільність використання таймерних сигналів для синтезу шумоподібних сигналів пояснюється можливістю таймерного кодування формувати значну кількість різних множин реалізацій $N_{\text{рТСК}}$ в залежності від параметрів m , s та i ,

що є основою для підвищення прихованості сигнальних конструкцій. З цього приводу доцільним є аналіз кожного з цих параметрів і надання оцінки їх впливу на наступні властивості: складність реалізації сигнальних конструкцій, завадостійкість, прихованість.

Параметр m визначає розмірність базового алфавіту тривалостей, з яких складаються таймерні сигнали. Зі зростанням m збільшується кількість можливих комбінацій формування сигналів на інтервалі $T_c = m \cdot t_0$. Однак суттєве збільшення m ускладнює реалізацію апаратної або програмної схеми генерації та декодування, що може обмежувати застосування таймерних сигналів в реальному часі.

Параметр s визначає тривалість інтервалу Δ , на основі якого задається тривалість імпульсу таймерного сигналу з урахування значення t_0 . Значення параметра в значній мірі впливає на можливість забезпечення структурної прихованості та завадостійкості. Менші значення s підвищують точність системи синхронізації, що підвищує завадостійкість, проте зменшує показник структурної прихованості. Великі значення s дозволяють формувати більш варіативні структури таймерного коду, забезпечуючи більші значення структурної прихованості. Проте, при цьому потрібно вирішувати більш складні завдання по забезпеченню стабільної системи циклової і тактової синхронізації. Це покращує прихованість та завадостійкість, особливо в умовах наявності перешкод і навмисного сканування спектру.

Параметр i визначає кількість ЗММ, значення яких може бути фіксованим або змінним. При випадковому або псевдовипадковому виборі цього параметра забезпечується непередбачуваність структури сигнальної конструкції, що підвищує структурну прихованість ТСК та ускладнює виявлення структури сигналу при дешифруванні.

Отже, комбінація параметрів m , s , та i дозволяє керовано варіювати властивості шумоподібного сигналу, зокрема:

1) складність реалізації сигнальних конструкцій зростає зі збільшенням розмірності алфавіту та зменшенням кроку дискретизації;

2) завадостійкість покращується завдяки неперіодичності та розмитості спектрального представлення сигналу;

3) прихованість значно зростає при великій кількості реалізацій $N_{p_TСК}$, що у випадку перехоплення повідомлення, суттєво ускладнюється розпізнавання сигналу без знання структури таймерного кодування засобами РЕР;

4) використання методу розширення спектра таймерного сигналу підвищує структурну та енергетичну прихованість шумоподібного сигналу.

З урахуванням зазначеного, доцільно використовувати адаптивний підхід до вибору параметрів ТСК залежно від характеристик каналу зв'язку, рівня завад і вимог до рівня безпеки передавання інформації.

5.2. Порівняльний аналіз алгоритмів розширення спектра позиційних та таймерних сигналів

У системах захисту інформації застосування методів розширення спектра сигналів відіграє ключову роль у підвищенні їх завадостійкості та прихованості. Традиційно ці методи реалізуються на основі позиційних кодів, де інформація передається у визначених часових або частотних позиціях, що забезпечує контрольовану спектральну структуру сигналу. Водночас використання ТСК створює принципово інший підхід, де розширення спектра досягається завдяки варіації часових інтервалів між імпульсами, що забезпечує більш складну структуру шумоподібних сигналів [95-97]. Саме відмінності в алгоритмах і складності реалізації цих двох підходів визначають доцільність їх використання в умовах різних каналів зв'язку та сценаріїв протидії радіоелектронним загрозам.

При позиційних кодах інформація передається у вигляді послідовності імпульсів із фіксованою тривалістю біту t_0 . Саме цей часовий інтервал визначає базову дискретизацію сигналу та використовується для реалізації алгоритмів розширення спектра. При цьому, кожен інформаційний біт займає

чітко визначену часову позицію, що дозволяє застосовувати різні методи модуляції та спектрального розширення.

Модуляція для позиційного коду здійснюється з урахуванням одного або кількох інформаційних бітів із фіксованою тривалістю тактового інтервалу t_0 . Такий підхід забезпечує формування сигналів, у яких інформація кодується положенням імпульсу в часовій або частотній області. Використання багато-позиційних методів модуляції дозволяє суттєво підвищити питому швидкість модуляції $\gamma_{\text{пшм}}$, оскільки за один тактовий інтервал t_0 може передаватися не один, а кілька бітів інформації. Якщо кількість можливих позицій позначити через M , то кількість інформаційних бітів, що передаються за один символ, дорівнює:

$$k_6 = \log_2 M. \quad (5.1)$$

Відповідно, швидкість передавання інформації при позиційному кодуванні визначається як [51]:

$$\gamma_{\text{пшм}} = \frac{k_6}{t_0} = \frac{M}{t_0}. \quad (5.2)$$

При використанні модуляції таймерного сигналу потрібно враховувати алгоритм формування імпульсів сигнальної конструкції, тобто [51]:

$$t_c = t_0 + k\Delta, \quad k \in 0, 1, \dots, I, \quad t_0 > \Delta. \quad (5.3)$$

При цьому, характерним є те, що $\Delta = t_0/s$, тобто менше значення t_0 в s разів. Це принципово відрізняє таймерні сигнали від позиційних кодів, де фіксованою основою для модуляції є весь інтервал t_0 . Це означає наявність відмінності використання для таймерних сигналів методів модуляції які характерні для позиційних кодів.

У випадку модуляції ТСК вибір параметра Δ безпосередньо впливає на кількість можливих станів модуляції. Наприклад, для різних видів фазової модуляції [51, 98]:

1) ФМ-2 (BPSK) достатньо використання одного часового інтервалу Δ , який забезпечує два фазових стани;

2) ФМ-4 (QPSK) або КАМ-4 (QAM-4) потрібно щонайменше два часових інтервали Δ , що формують чотири можливі комбінації;

3) КАМ-16 (QAM-16) кількість необхідних інтервалів зростає до чотирьох, що дозволяє реалізувати 16 станів сигналу:

$$M_{\text{см}} = 2^{k_{\Delta}}, \quad t_M = \Delta \times k_{\Delta}, \quad (5.4)$$

де $M_{\text{см}}$ – кількість станів модуляції, k_{Δ} – кількість часових інтервалів, що використовуються для модуляції, t_M – інтервал часу для модуляції елементів Δ .

Отже, при використанні багатопозиційної модуляції для таймерних сигнальних конструкцій реалізується масштабування базового інтервалу t_0 на дробові частини Δ . Це створює передумови для формування більш складних шумоподібних сигналів, які характеризуються підвищеною ентропією та спектральною насиченістю. Завдяки цьому досягається зростання структурної прихованості, що суттєво ускладнює несанкціонований аналіз структури сигналів та підвищує їх стійкість до методів радіоелектронної розвідки.

Дамо аналіз модуляції позиційних та таймерних сигналів з точки зору частотної ефективності, яка визначається кількістю інформаційних бітів, що передаються в одиниці смуги частот:

$$\gamma = \frac{R}{\Delta F}, \quad (5.5)$$

де R – швидкість передавання даних, ΔF – ширина смуги сигналу.

Для позиційних кодів смуга визначається оберненою величиною від t_0 :

$$\Delta F_{\text{ПК}} \approx \frac{1}{t_0}, \quad \gamma_{\Delta F_{\text{ПК}}} = R_{\text{ПК}} \times t_0. \quad (5.6)$$

Для ТСК через введення дробових інтервалів Δ смуга не зменшується, а залежить від тривалості імпульсів t_c :

$$\Delta F_{\text{ТСК}} \geq \frac{1}{t_c} = \frac{1}{t_0 + k\Delta}, \quad \gamma_{\Delta F_{\text{ПК}}} \geq R_{\text{ТСК}} \times t_0. \quad (5.7)$$

Тобто частотна ефективність таймерних сигналів в залежності від параметрів m , s , та i співпадає або більше ніж у позиційних кодів:

$$\gamma_{\Delta F_{\text{ТСК}}} \geq \gamma_{\Delta F_{\text{ПК}}} \quad (5.8)$$

за умови, що $\Delta F_{\text{ТСК}} = \Delta F_{\text{ПК}}$.

Розглянемо розширення спектра промодульованого таймерного сигналу. У задачах синтезу сигналів із заданими статистичними та спектральними властивостями [99, 100], як правило, використовуються системи ортогональних функцій. До таких систем належать ортогональні поліноми Чебишева, Лагерра, Лежандра та інші, які дозволяють будувати узагальнені базиси для формування сигналів. У вітчизняній та зарубіжній літературі детально досліджено питання синтезу ортогональних і квазіортогональних сигналів. Значний внесок у розвиток цього напрямку зробили Є. Наумов, В. Бичков, М. Мазурков, О. Скопа, Н. Казакова, Б. Радзимоський та інші [17, 18, 99-102]. Їхні роботи заклали фундаментальні підходи до побудови шумоподібних сигналів.

Шумоподібний сигнал можна розглядати як послідовність імпульсів або гармонік, вагові коефіцієнти яких формуються за псевдовипадковим законом. У загальному випадку сигнал подається як розклад у базисі ортогональних функцій:

$$s(t) = \sum_{k=1}^{N_{\text{pn}}} a_k \varphi_k(\tau), \quad (5.9)$$

де a_k – вагові коефіцієнти, що формуються за законом випадковості або псевдовипадковості, $\varphi_k(\tau)$ – ортогональні або квазіортогональні базисні функції, $N_{\text{рп}}$ – розмірність простору сигналу.

У випадку використання ПВП для кодування інформації, сигнал набуває властивостей, близьких до білого шуму. Зокрема, для кореляційної функції $K_s(\tau)$ виконується умова:

$$K_s(\tau) \approx \begin{cases} 1, & \tau = 0, \\ 0, & \tau \neq 0, \end{cases} \quad (5.10)$$

що забезпечує низьку взаємну кореляцію сигналів і високу ефективність при застосуванні в системах з розширеним спектром. Основними факторами, які впливають на захист інформації від засобів радіоелектронної розвідки є низький рівень спектральної щільності потужності шумоподібного сигналу, що сприяє підвищенню енергетичної прихованості та завадостійкості.

До основних методів синтезу шумоподібних сигналів на основі позиційних кодів використовуються ортогональні або квазіортогональні послідовності, псевдовипадкових перескок робочої частоти, лінійна частотна модуляції, а також комбіновані методи. Як правило, для всіх відомих методів розширення спектра бінарної послідовності використовується базовий елемент t_0 .

При використанні таймерних сигналів при розширенні спектра потрібно враховувати часові побудови сигнальних конструкцій n , s , i та Δ . Це потребує інших алгоритмів для синтезу шумоподібних сигналів [97-99].

У випадку позиційного кодування розширення спектра здійснюється шляхом використання фіксованого тактового інтервалу t_0 . Основні методи ґрунтуються на накладанні інформаційної послідовності на одну з відомих шумоподібних структур, що формуються за допомогою ортогональних або

квазіортогональних функцій. Для бінарної послідовності $b_i \in \{0, 1\}$ це можна записати як:

$$s_{\text{пк}}(t) = b_{\text{пк}}(t) \sum_{i=1}^N b_k \varphi(t - it_0), \quad (5.11)$$

де $\varphi(\tau)$ – базовий елемент розширення спектра позиційного сигналу, t_0 – фіксована тривалість тактового імпульсу.

Представлена модель (5.11) дозволяє визначити положення кожного біта в часі, а спектр позиційного сигналу розширюється за рахунок зміну стану псевдовипадкових імпульсів.

Для таймерних сигнальних конструкцій модель розширення спектра відрізняється, що пов'язано з непозиційністю імпульсів t_c по відношенню до базового часового елементу t_0 . Тут часова структура сигналу визначається не тільки тактом t_0 , але й додатковим часовим параметром $\Delta = t_0/s$, що дозволяє формувати імпульси за певної умови $t_c = t_0 + k\Delta$ ($k \in 0, 1, \dots, I, t_0 > \Delta$).

Розглянемо модель таймерного сигналу з накладанням ПВП на весь інтервал $T_{\text{тск}} = m \cdot t_0$. Нехай базова ТСК має складатися з m тактових інтервалів t_0 , а $c(t)$ – ПВП (PN-код), яка визначена на всьому інтервалі $T_{\text{тск}}$. Позначимо кількість чипів ПВП, що укладаються в $T_{\text{тск}}$, через $L_{\text{тск}}$. Тривалість одного чипа

$$\tau = \frac{T_{\text{тск}}}{L_{\text{тск}}}. \quad (5.12)$$

Швидкість чипів оцінюється за формулою:

$$R_\tau = \frac{1}{\tau} = \frac{L_{\text{тск}}}{m \cdot t_0}. \quad (5.13)$$

Кількість чипів на один базовий інтервал t_0 :

$$\ell = \frac{t_0}{\tau}. \quad (5.14)$$

Загальна кількість чіпів ПВП на інтервалі часу :

$$L_\tau = m \times \ell. \quad (5.15)$$

Коефіцієнт розширення спектра в цьому випадку становить:

$$G = \frac{R_\tau}{R_b} = \frac{t_0}{\tau} = \ell, \quad (5.16)$$

де $R_b = 1/t_0$ – бітова швидкість передавання даних.

З урахуванням структури таймерного сигналу і накладанням ПВП модель шумоподібного таймерного сигналу можна представити у вигляді:

$$s_{\text{ТСК}}(t) = \sum_{j=1}^{N_s} b_j \cdot c_j(t) \left[\sum_{g=1}^m A_{j,g} \varphi(t - T_{j,g}) \right], \quad (5.17)$$

де $T_{j,g} = t_{j,0} + (g - 1)t_0 + k_{j,g}\Delta$, $t \in [t_{j,0}, t_{j,0} + T_{\text{ТСК}}]$, b_j – j -й інформаційний блок бітів, $c_j(t)$ – ПВП, визначена на інтервалі часу $T_{\text{ТСК}}$, $A_{j,g}$ – амплітуда g -го елемента, $\varphi(t)$ – форма елементарного імпульсу, $k_{j,g}$ – дискретний коефіцієнт зсуву імпульсу ТСК.

Множення у часі на ПВП $c_j(t)$ відповідає згортці спектрів у частотній області. Нехай $S_{\varphi,T}(f)$ – спектр таймерної імпульсної структури $\sum_{g=1}^m A_{j,g} \varphi(t - T_{j,g})$, а $C(f)$ – спектр ПВП. Тоді спектр одного блоку:

$$S_{\text{ТСК}}(f) = S_{\varphi,T}(f) \times C(f). \quad (5.18)$$

Оскільки $C(f)$ широкосмуговий складова при великому значенні швидкості R_τ , згортка сприяє розсіюванню енергії по ширшій смузі частот, що забезпечує розширення спектра сигналу.

Автокореляція функція сигналу згідно моделі (5.17) записується як згортка відповідних автокореляцій:

$$R_s(\tau) = R_\tau(\tau) \times R_{\varphi,T}(\tau), \quad (5.19)$$

де $R_\tau(\tau)$ – КФ ПВП (має вигляд піку при $\tau=0$), $R_{\varphi,T}(\tau)$ – АКФ таймерної імпульсної структури.

Якщо ПВП має властивість «дельта-подібної» АКФ, тобто наявність невеликих бокових пелюстків, то сумарний $R_s(\tau)$ матиме зменшені бокові пелюстки і покращується квазіортогональність і селективність кореляційного прийому. В ідеальному наближенні для якісної оцінки отримаємо наступне:

$$R_s(\tau) \approx \begin{cases} \ell, & \tau = 0, \\ 0, & \tau \neq 0. \end{cases} \quad (5.20)$$

Для практично аналізу (5.19) можна представити у нормованому вигляді:

$$R_s(\tau) \approx \begin{cases} 1, & \tau = 0, \\ \frac{1}{\ell}, & \tau \neq 0. \end{cases} \quad (5.21)$$

Графік автокореляційної функції (АКФ) для псевдовипадкової послідовності розширення спектра надано на рис. 5.1 .

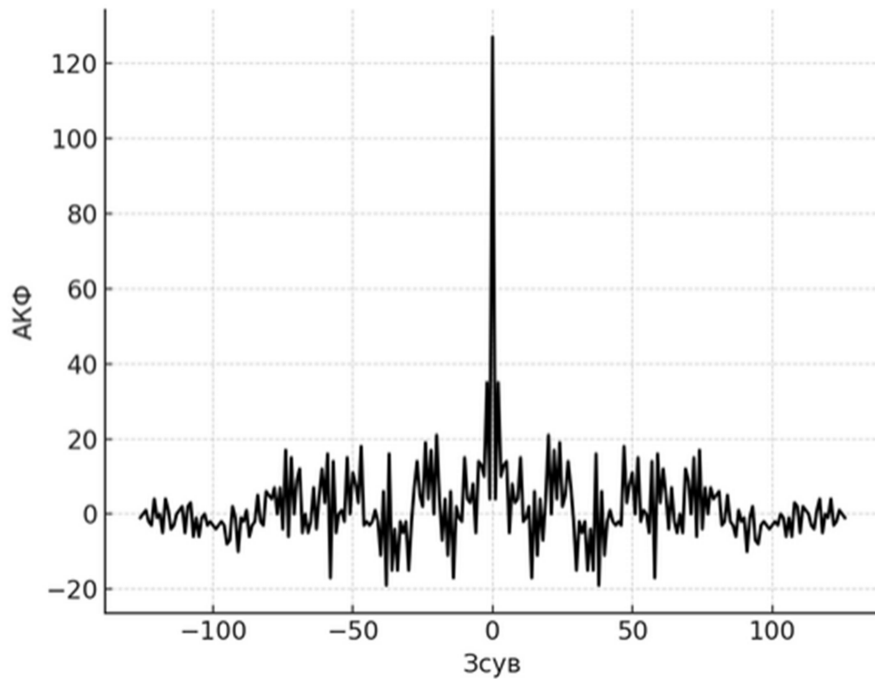


Рисунок 5.1– Графік АКФ для ПВП розширення спектра

Гострий пік АКФ ПВП у нульовій затримці $\tau = 0$ відображає повну кореляцію послідовності із самою собою. Малі значення для ненульових затримок свідчать про відсутність повторюваних закономірностей і забезпечують властивості шумоподібного сигналу. Енергетична прихованість забезпечується завдяки тому, що сигнал розподілений у широкій смузі частот та він має низьку спектральну щільність потужності. Висока розрізнявальна здатність пояснюється завдяки близькості АКФ до дельта-функції, що забезпечує в системах з розширеним спектром вирішення задачі синхронізації та виявлення сигналу. Отже, АКФ ПВП є ключовою характеристикою, що обґрунтовує їх використання для розширення спектра сигналів у системах зв'язку та захисту інформації.

Слід відзначити, що ПВП розширення спектра на інтервалі часу $T_{\text{тск}} = m \cdot t_0$ повністю «покривала» таймерну конструкцію, слід обирати τ так, щоб $L_\tau = mt_0/\tau$ було ціли. На практиці допускають нескладні нечіткі співвідношення і вирівнювання чипів по межах тактів. Обмеження фізичного каналу, яка зі смугою пропускання ΔF , накладає вимогу на мінімальну тривалість чипа: $\tau \geq 1/2\Delta F$ з урахуванням умови Найквіста. Збільшення $G = \ell$

забезпечує підвищення прихованості та завадостійкості, але ускладнює синхронізацію та збільшує вимоги до апаратури приймача.

АКФ таймерних імпульсних структур суттєво відрізняється від АКФ ПВП, оскільки тут використовується змінна тривалість імпульсів, яка задається умовою $t_c = t_0 + k\Delta$ ($k \in 0, 1, \dots, l, t_0 > \Delta$).

У загальному випадку автокореляційна функція імпульсів ТСК визначається як:

$$R_{\text{ітск}} = \frac{1}{T_{\text{тск}}} \int_0^{T_{\text{тск}}} s_{\text{ітск}}(s) s_{\text{ітск}}(t + \Delta) dt. \quad (5.22)$$

Графік АКФ таймерної сигнальної конструкції надано на рис. 5.2. Багаторівнева структура АКФ на відміну від ПВП, де спостерігається майже дельта-подібна форма, АКФ ТСК має кілька локальних максимумів, зумовлених накладанням дробових інтервалів Δ .

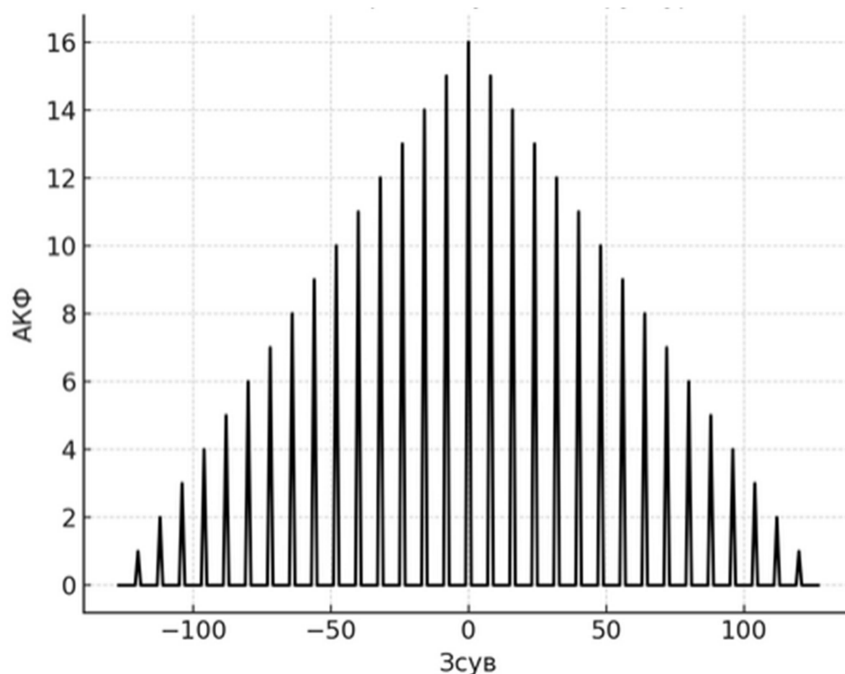


Рисунок 5.2 – Графік АКФ таймерної сигнальної конструкції

Менша регулярність бокових пелюсток забезпечує можливість підвищення структурної прихованості сигналу. Розширений спектр за рахунок

дробового масштабування t_0 ускладнює визначення структури сигналу засобами радіоелектронної розвідки. Залежність від параметрів n , s , i та Δ дозволяє варіювати кореляційні властивості та формувати множину сигнальних реалізацій з різною завадостійкістю.

Таким чином, АКФ таймерної імпульсної структури має складніший вигляд, ніж у АКФ ПВП, що обумовлює підвищену структурну прихованість сигналів у системах із розширеним спектром, але водночас ускладнює задачу синхронізації.

5.3. Вибір розрядності таймерного кодування

При вирішенні завдання синтезу таймерних шумоподібних сигналів [59, 69, 76, 77, 103, 104] важливим є обґрунтований вибір параметрів побудови ТСК. Таймерне кодування дозволяє формувати значну кількість різних множин реалізацій N_p в залежності від параметрів m , s та i , що є основою для підвищення прихованості сигнальних конструкцій. З цього приводу доцільним є аналіз кожного з цих параметрів і надання оцінки їх впливу на наступні властивості: складність реалізації сигнальних конструкцій, завадостійкість, прихованість.

Важливим показником побудови ТСК є вибір кількості інтервалів Найквіста m для побудови сигнальних конструкцій. Часовий інтервал побудови таймерних сигналів T_c задається певною кількістю інтервалів Найквіста m . На рис. 5.3 наведені залежності реалізації N_p для множин ТСК1 ($s=7$, $i=4$), ТСК2 ($s=6$, $i=4$), ТСК3 ($s=5$, $i=4$), ТСК4 ($s=4$, $i=4$) від кількості інтервалів Найквіста m . Також на рис. 5.3 надана залежність кількості реалізацій для РЦК.

Бачимо, що потужність таймерних сигналів по можливості формування кількості комбінацій суттєво перевищує реалізації РЦК. Побудовані закономірності реалізацій таймерних сигналів дозволяють зробити висновок, що збільшення кількості m дозволяє суттєво збільшити число реалізацій N_p . Наприклад, для $m=6$, $s=5$, $i=4$ можна побудувати $N_{\text{ртск}}=1001$ реалізацій ТСК.

При підвищенні кількості інтервалів Найквіста до $m=19$ та при незмінних $s=5$, $i=4$ можна побудувати значно більшу кількість реалізацій $N_p = 1502501$. Структурна прихованість згідно (3.1) $S_{\text{тск}}(m=6, s=5, i=4)=9,96$ дв.вим та суттєво підвищується при збільшенні значення m та складає $S_{\text{тск}}(m=19, s=5, i=4)=20,5$ дв.вим.

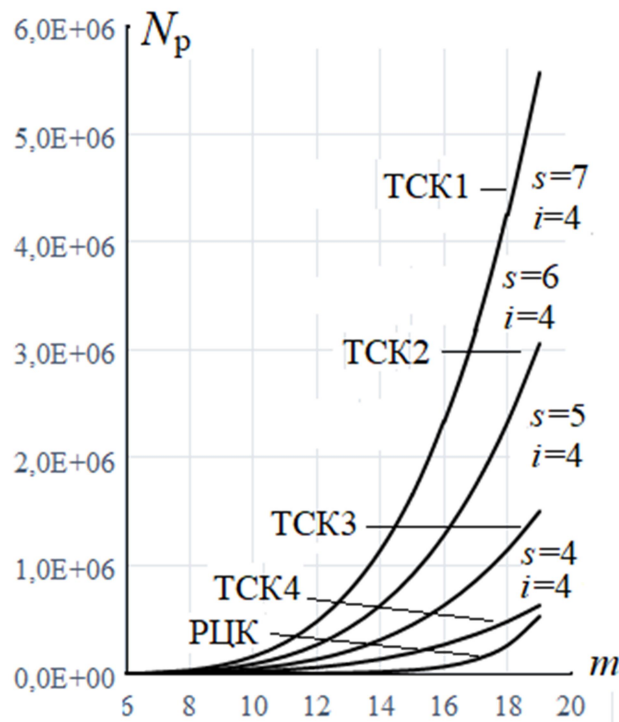


Рисунок 5.3 – Залежності N_p від m , s та i

Такий підхід побудови сигнальних конструкцій за допомогою кількості інтервалів m не суперечить умові забезпечення максимально можливого значення структурної прихованості, проте збільшуються вимоги до точності реєстрації значущих моментів відновлення (ЗМВ) в приймачі. З цього приводу доцільним є обмеження кількості інтервалів m , а збільшення числа реалізацій $N_{\text{ртск}}$ пропонується за рахунок зміни параметрів s та i .

5.4. Оцінка числа реалізації за рахунок збільшення значущих моментів модуляції таймерного сигналу

Розглянемо можливості збільшення числа реалізацій за рахунок використання ТСК [61, 93-95] з різним числом ЗММ i . На рис. 5.4 надано залежності N_p від i , m та $s=5$, за якими можна побачити максимальні значення кількості реалізацій за певним значенням ЗММ. Так для $m=8$ максимальне значення реалізацій $N_p=15504$ досягається при $i=5$, для $m=10$ отримуємо $N_p=230230$ при $i=6$. Отже, при виборі параметрів ТСК для завдання розширення спектра обґрунтованим є вибір оптимального значення $i_{\text{опт}}$, при якому забезпечується максимальне значення реалізацій та структурної прихованості, тобто:

$$\max N_p = S\{i_{\text{опт}}, n, s, P_{\text{НП}}(n)\}. \quad (5.23)$$

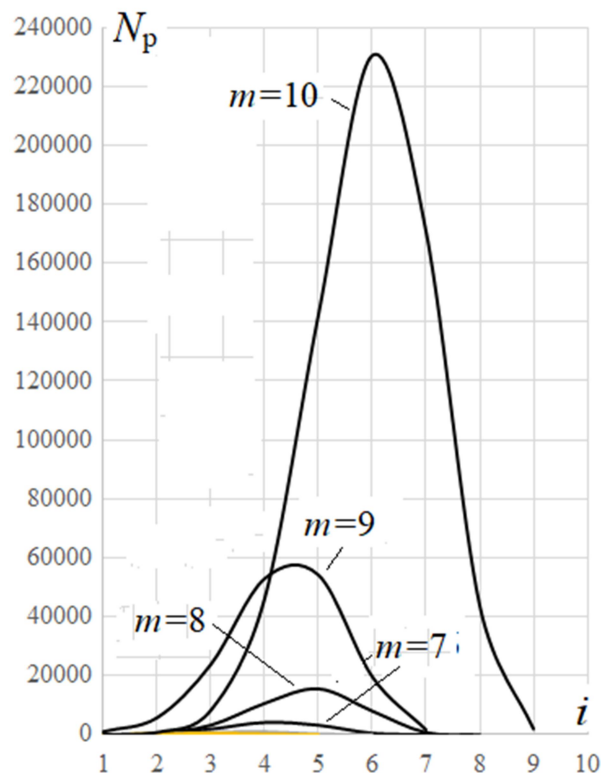


Рисунок 5.4 – Залежності N_p від i , m та $s=5$

Проте можливо використання множин комбінацій, в яких значення i буде змінюватися від одного до $m - 1$ (табл. 5.1). Це суттєво збільшить ансамбль реалізацій N_p та підвищить структурну прихованість, тобто:

$$\max N_{p\Sigma} = S\{i = 1, 2, \dots, m - 1, m, s, P_{\text{НП}}(n)\}. \quad (5.24)$$

Умова (5.24) використовує сумарне значення реалізацій ТСК з різною кількістю ЗММ. В табл. 5.1 наведено результати отриманої кількості реалізацій в залежності від m, s та $i = 1, 2, \dots, m - 1$.

Таблиця 5.1 – Кількість сумарних реалізацій таймерних сигналів $N_{p\Sigma}$ при $i = 1, 2, \dots, m - 1$

m	s			
	3	4	5	6
5	188	344	570	881
6	594	1251	2327	3969
7	1872	4543	9495	17886
8	5895	16492	38739	80607
9	18533	59829	38739	363203
10	58424	217285	644760	1636943

Бачимо, що досягнути достатньої кількості комбінацій можливо не за рахунок збільшення кількості інтервалів Найквіста, а за допомогою об'єднання реалізацій з різним числом ЗММ при фіксованому значенні m .

5.5. Оцінка впливу базового елементу побудови таймерного сигналу на кількісні і якісні показники передавання інформації

Розглянемо варіант збільшення числа реалізацій за рахунок підвищення значення s . На рис. 5.5 надано залежності N_p від s , m , $i=3$, з яких можна побачити, що з ростом часових інтервалів s суттєвого збільшується кількість комбінацій ТСК, а також спостерігається підвищення структурної прихованості. Проте, при збільшенні s зменшується часовий інтервал Δ і за певних значеннях $s=\text{const}$ та m можна досягти максимальне значення пропускної здатності каналу [32]:

$$C_{\text{ТСК}} = \frac{\log_2 N_p - \bar{i} H_3 \left(\frac{z_i}{k_i} \right) - H_3}{m}, \quad (5.25)$$

де H_3 – ентропія на прийомі таймерних сигналів, яка визначається як:

$$H_3 = - \left[p_B \log_2 p_B + (1 - p_B) \log_2 \frac{(1-p_B)}{N_p-1} \right], \quad (5.26)$$

p_B – ймовірність вірного прийому таймерних сигналів; $H_3 \left(\frac{z_i}{k_i} \right)$ – умовна ентропія, яка характеризує невизначеність ймовірності сигнальної конструкції з k -переходами за умови, що приймач отримав сигнал з i -переходами та визначається як:

$$H \left(\frac{z_i}{k_i} \right) = - \sum_{i=1}^{Z_0} P \left(\frac{z_i}{k_i} \right) \log_2 P \left(\frac{z_i}{k_i} \right),$$

де: $P \left(\frac{z_i}{k_i} \right)$ – ймовірність одержання зменшення ЗМВ переходу на $z\Delta$. Залежності пропускної здатності каналу з різним рівнем флуктуаційних шумів ($h = u_c/u_3$) та величини s надано на рис. 5.6.

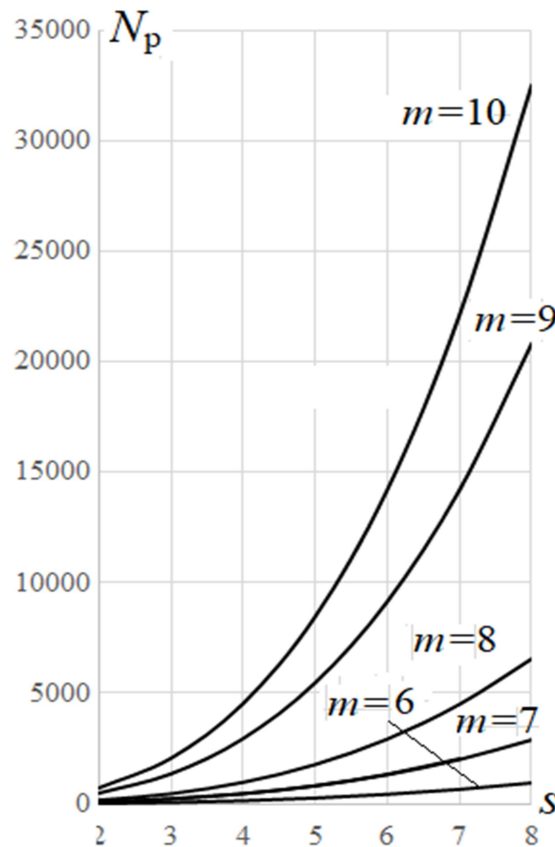


Рисунок 5.5 – Залежності N_p від s , m , $i=3$

Залежності під номерами 1...3 побудовані для значень $h = 7,5$ і $m = 8, 6, 5$ відповідно, під номерами 4...6 для $h = 5,5$ і $m = 8, 6, 5$ відповідно. Залежності 1, 2, ... 6 дають зрозуміти, що при виборі параметру s , потрібно враховувати умову забезпечення максимальної пропускної здатності. Для залежності 4, 5 та 6 отримуємо оптимальне значення $s_{\text{опт1}} = 6$, при якому забезпечується максимальне значення $C_{\text{тск}}$. Для залежності 1, 2 та 3 отримуємо $s_{\text{опт2}} = 8$. За умови $s > s_{\text{опт}}$ зменшується часовий інтервал Δ , що призводить до збільшення показника H_3 , який характеризує втрати із-за збільшення спотворених сигнальних конструкцій. Отже, виявлено протиріччя між умовою підвищення структурної прихованості шляхом збільшення s та необхідністю обмеження цього показника значенням $s \leq s_{\text{опт}}$ при заданому m та відношенням сигнал/шум h .

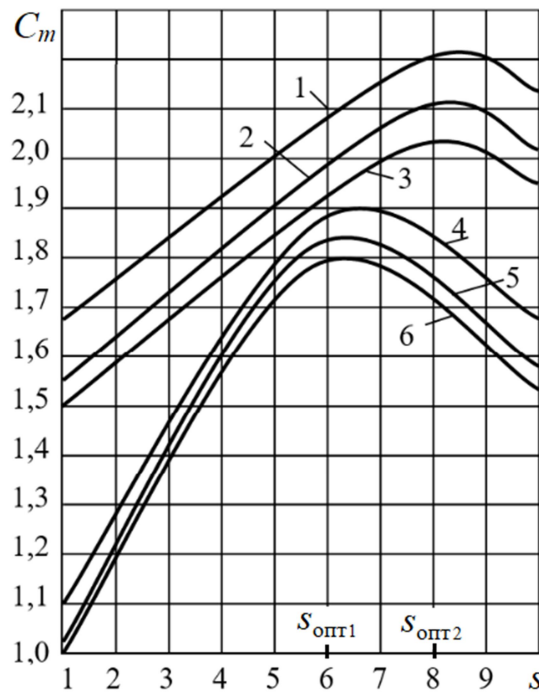


Рисунок 5.6 – Залежності пропускної $C_m = f(s)$ при $h = \text{const}$, $m = \text{const}$

Таким чином, ці дослідження дали змогу визначити основні вимоги по вибору параметрів таймерних сигналів для завдання формування шумоподібних сигналів за допомогою різних методів розширення спектра. Визначено обмеження на вибір параметрів ТСК, які впливають на складність реалізації шумоподібних таймерних сигналів, їх передавання та прийому, забезпечення завадостійкості та прихованості.

5.6. Генерування псевдовипадкових послідовностей з підвищеною криптографічної стійкістю

5.6.1. Оцінка якості псевдовипадкових послідовностей

Захист переданої інформації від несанкціонованого доступу в сучасних інформаційно-комунікаційних системах здійснюється на різних рівнях моделі OSI за допомогою криптографічних методів та шумоподібних сигналів. Протистояння криптографії й криптоаналізу свідчить, що з часом криптографічна стійкість будь-якої системи зменшується, а її компрометація

стає питанням часу. Тому підтримання високого рівня захищеності можливе лише за рахунок постійного вдосконалення методів шифрування та механізмів формування псевдовипадкових послідовностей.

Псевдовипадкові послідовності мають подвійне призначення [17, 78, 100]: вони використовуються для побудови криптографічних алгоритмів та для розширення спектра цифрових сигналів з метою створення шумоподібних сигналів. Саме ці сигнали визначають показники енергетичної та структурної прихованості передавання. Очевидно, що якість генераторів псевдовипадкових чисел безпосередньо впливає як на криптографічну стійкість систем шифрування, так і на прихованість сигналів у системах зв'язку.

У криптографічних системах традиційно застосовуються лінійно-конгруентні генератори, основним недоліком яких є обмежений період формування числових послідовностей. Це обмежує їх придатність для побудови сучасних систем захисту. На відміну від них, генератори хаосу, що базуються на використанні явищ динамічного хаосу, мають суттєві переваги. Період вибірки у таких генераторах визначається розрядністю обчислювальної системи, що дозволяє отримувати значно довші послідовності. Впровадження хаотичних систем у сферу інформаційної безпеки та інфокомунікаційних технологій відкрило нові можливості для синтезу сигнально-кодових конструкцій з високою прихованістю, а також створення криптосистем із підвищеною стійкістю.

Однак для практичного застосування генераторів хаосу необхідна детальна оцінка їх статистичних характеристик. Очевидно, що якість таких генераторів повинна перевірятися за допомогою стандартних статистичних тестів, зокрема системи NIST. Дослідження показують, що не всі хаотичні генератори повністю задовольняють вимоги NIST, що зумовлює потребу у вдосконаленні методів їх побудови.

Для статистичної оцінки якості згенерованих бінарних послідовностей застосовано систему тестів NIST SP 800-22. Основним критерієм виступає

ймовірність χ^2 , яка дозволяє визначити відповідність послідовності вимогам випадковості. Ключові етапи методики полягають в наступному:

- 1) формування бінарних вибірок із використанням кожного з хаотичних відображень;
- 2) тестування за допомогою 16 базових тестів NIST;
- 3) аналіз результатів відхилення χ^2 від довірчого інтервалу $[0,05; 1]$.

Проведемо порівняльний аналіз різних типів генераторів хаосу для завдання формування бінарних псевдовипадкових послідовностей. За результатами тестування визначимо генератори з найкращими статистичними властивостями, а також потрібно запропонувати методи поліпшення якості реалізацій послідовностей.

5.6.2. Тестування та вимоги до псевдовипадкових послідовностей

Псевдовипадкові послідовності, сформовані на основі генераторів динамічного хаосу, повинні відповідати статистичним вимогам, що пред'являються до випадкових процесів. Динамічний хаос [107-112] характеризується всіма ключовими властивостями випадковості, а саме нерегулярністю, аперіодичністю та чутливістю до початкових умов. Навіть незначна зміна параметрів хаотичної системи призводить до істотних відмінностей у траєкторії її еволюції, що забезпечує практично необмежену кількість різних псевдовипадкових послідовностей. Саме ця властивість робить хаотичні генератори перспективними для задач криптографії та побудови шумоподібних сигналів.

Для криптографічних застосувань найбільш доцільним є використання генераторів із рівномірним законом розподілу чисел [113-115]. Вони функціонують за певним алгоритмом, де кожне наступне число визначається на основі попереднього. Такий підхід має низку переваг:

- 1) можливість попереднього відбору вибірки з перевіреними статистичними властивостями, що гарантує стабільність та знижує потребу в регулярному тестуванні;
- 2) забезпечення відтворюваності послідовності з довільної позиції;
- 3) мінімальна обчислювальна складність формування наступного елемента;
- 4) низькі вимоги до обсягу пам'яті;
- 5) довжина періоду не менша за заданий для конкретного процесу.

Дослідження показують [113], що пошук вибірок із необхідними статистичними властивостями є складною задачею і потребує значних обчислювальних витрат. Саме тому для перевірки генераторів випадкових та псевдовипадкових чисел застосовуються спеціальні статистичні критерії [3], серед яких: критерій Пірсона, Колмогорова–Смирнова, Стюдента та інші. Найбільш універсальним вважається критерій Критерій Пірсона χ^2 , який не залежить від закону розподілу випадкової величини [57]:

$$\chi^2 = \sum_{i=1}^k \frac{(Q_i - E_i)^2}{E_i}, \quad (5.27)$$

де Q_i – кількість спостережень у i -му інтервалі, E_i – очікувана кількість спостережень, k – кількість інтервалів.

Цей критерій має широкі можливості для аналізу випадкових величин, сигналів і послідовностей. Його основна ідея полягає в перевірці відповідності експериментального розподілу ймовірностей теоретичному. У контексті інформаційної безпеки, криптографії та аналізу псевдовипадкових послідовностей цей критерій дозволяє:

- 1) перевіряти гіпотези про розподіл вибірки;
- 2) оцінювати рівномірності та випадковості вибірки, а також виявляти відхилення в статистичних властивостях сигналів та шифрованих даних;

3) виявляти кореляції та залежності, тобто, якщо результати відрізняються від рівномірного розподілу, це може свідчити про наявність закономірностей у сигналі, що знижує криптостійкість;

4) аналізувати якість шифрування, яке полягає в оцінці «близькості до випадковості» вихідного шифротексту, тобто, якщо χ^2 виходить за критичні межі, можна підозрювати недосконалість алгоритму.

5) виконувати порівняння декількох генераторів псевдовипадкових послідовностей для встановлення який з них забезпечує більш якісні показники.

5.6.3. Метод підвищення якісних показників реалізацій генераторів хаосу

Розглянемо метод підвищення якісних показників реалізацій хаотичних коливань [113-116]. Для проведення експерименту використано декілька дискретних відображень у генераторах хаосу:

1) степеневе відображення:

$$x_{n+1} = a(1 - |1 - 2x_n|^l), \quad (5.28)$$

де $x_0 = 0,8$, $a = 0,9$, $l = 0,8$;

2) логістичне відображення:

$$x_{n+1} = ax_n(1 - x_n), \quad (5.29)$$

де $x_0 = 0,9$, $a = 3,9$;

3) кубічне відображення:

$$x_{n+1} = (1 - 4a)x_n + 4ax_n^3, \quad (5.30)$$

де $x_0 = 0,5$, $a = 0,92$;

4) відображення типу зсуву:

$$x_{n+1} = ax_n \bmod 1 \quad (5.31)$$

де $x_0 = 0,8$, $a = 3,0$.

Для оцінювання статистичних властивостей сформованих бінарних послідовностей було використано систему тестів NIST, зокрема розглянуто значення ймовірності $P(\chi^2)$. На рис. 5.7-5.10 наведено результати тестування генераторів хаосу з різними відображеннями.

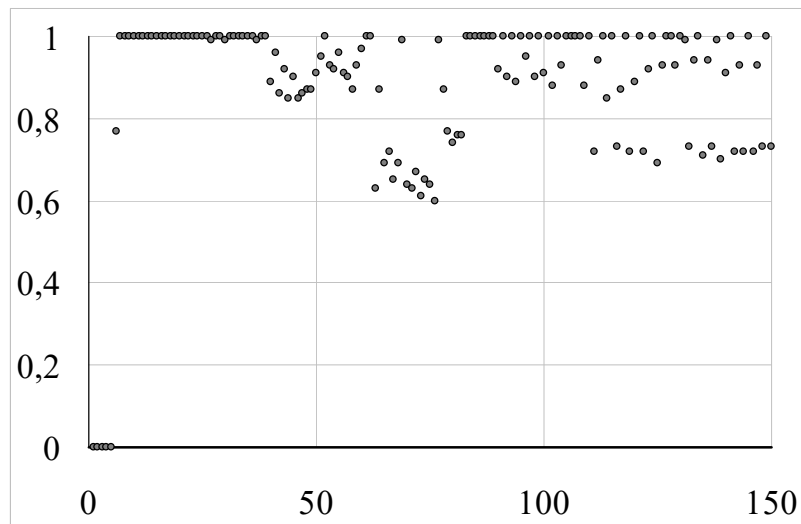


Рисунок 5.7 – Результати тестування степеневого генератора хаосу

Аналіз показав, що не всі реалізації відповідають вимогам випадковості:

1) генератори з логістичним (рис. 5.8), кубічним (рис. 5.9) та зсувним (рис. 5.10) відображеннями не проходять частину тестів NIST, оскільки для ряду отриманих вибірок значення $P(\chi^2) < 0,05$;

2) задовільні результати були отримані лише для степеневого генератора хаосу (рис. 5.7), який забезпечив проходження більшості тестів у межах довірчого інтервалу.

З метою підвищення стабільності статистичних характеристик було запропоновано комбінування кількох хаотичних генераторів. Для формування підсумкової бінарної послідовності використовувалася операція XOR. На рис.

5.11 наведено результати тестування послідовності, сформованої шляхом поєднання генератора типу зсуву та кубічного генератора.

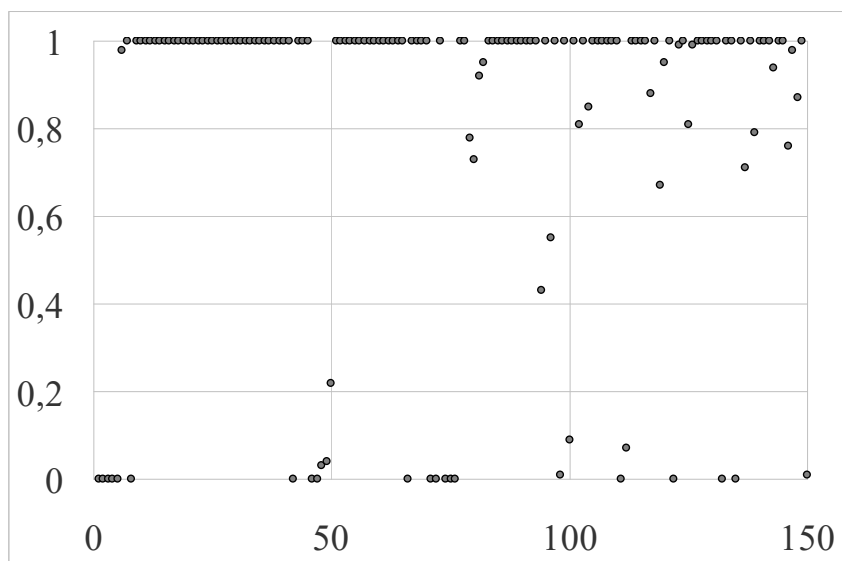


Рисунок 5.8 – Результати тестування генератора хаосу з логістичним відображенням

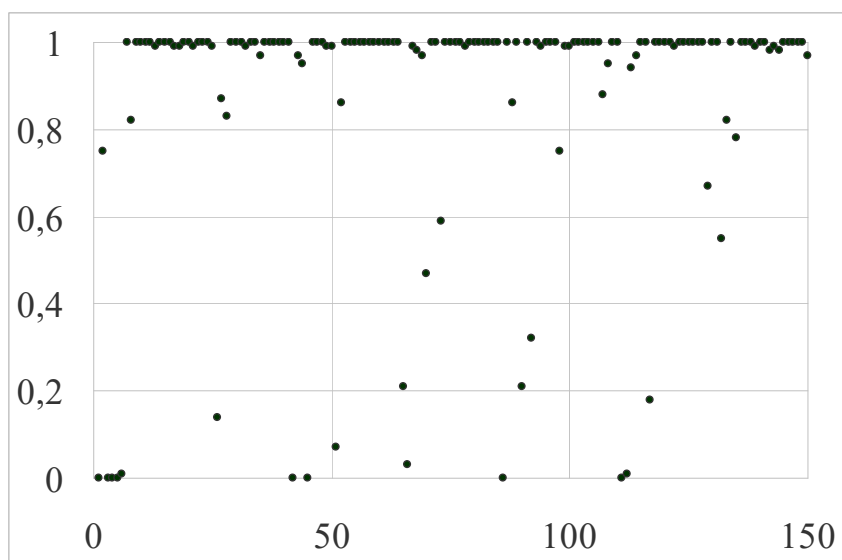


Рисунок 5.9 – Результати тестування генератора хаосу із кубічним відображенням

Отримані результати підтверджують, що якість вибірки значно покращилася: більшість тестів NIST було пройдено, а значення ймовірності

$P(\chi^2)$ знаходяться в межах довірчого інтервалу, тобто $P(\chi^2) > 0,05$. Це свідчить про ефективність використання кількох хаотичних генераторів при синтезі сумарних бінарних послідовностей для завдання стабілізації статистичних характеристик реалізації.

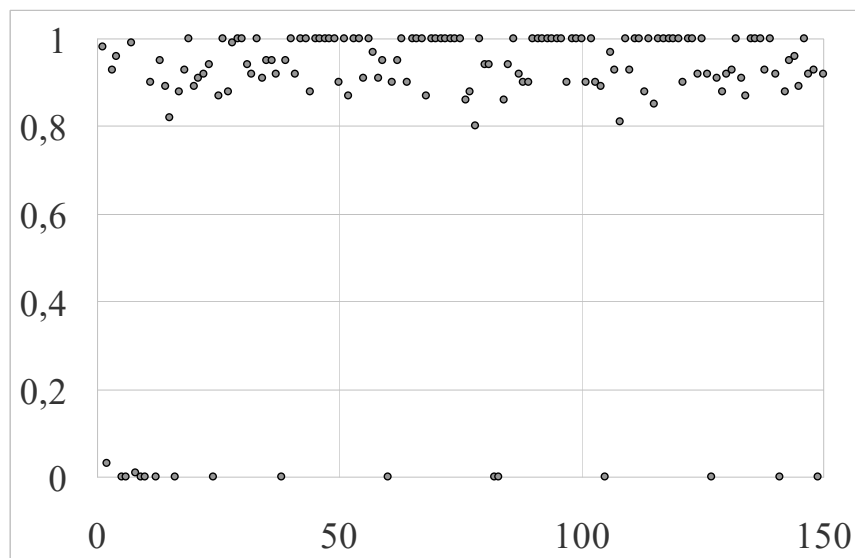


Рисунок 5.10 – Результати тестування генератора хаосу з відображенням типу зсуву

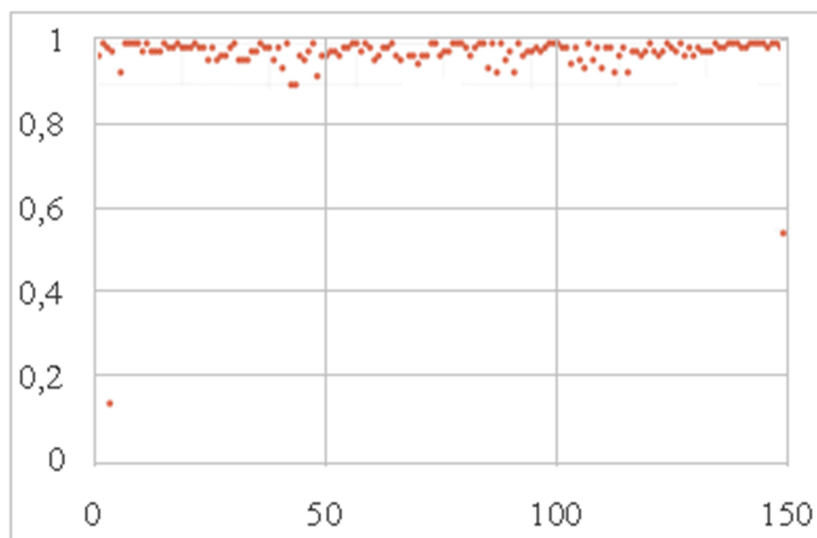


Рисунок 5.11 – Результати тестування послідовності, сформованої на основі генератора типу зсув та кубічного генератора

Отже, використання генераторів хаосу дозволяє створювати псевдовипадкові послідовності з покращеними статистичними

характеристиками, що підвищує як криптографічну стійкість систем шифрування, так і рівень прихованості шумоподібних сигналів у системах радіозв'язку.

5.6.4. Синтез послідовностей із підвищеною криптографічною стійкістю

Криптографічна стійкість систем шифрування безпосередньо залежить від рівня випадковості використовуваних числових послідовностей [113]. Якщо псевдовипадкова послідовність генератора задовольняє вимогам статистичних тестів, її можна вважати випадковою. Проте цього недостатньо для гарантування високої криптографічної стійкості алгоритму генерації псевдовипадкових чисел. Послідовність вважається криптографічно безпечною лише за умови, що вона має властивість непередбачуваності наступного елемента. Зазвичай таку характеристику мають генератори випадкових чисел.

У даному підрозділі розглянемо алгоритм формування псевдовипадкових послідовностей із підвищеною криптографічною стійкістю [113]. Метод ґрунтується на комбінованому використанні двох хаотичних генераторів і включає такі кроки:

1) за допомогою першого генератора хаосу формується множина псевдовипадкових чисел у інтервалі $]0; 1[$:

$$x_1, x_2, x_3, \dots, x_N; \quad (5.32)$$

2) інтервал $]0; 1[$ розбивається на z рівних підінтервалів (наприклад, $z = 2, 3, 4$ тощо);

3) Формується перше підмножина з z чисел. Наприклад, при $z = 3$ обираються числа x_1, x_2, x_3 , де x_1 відповідає першому підінтервалу, x_2 – другому, а x_3 – третьому;

4) Другий генератор хаосу формує псевдовипадкове число $y_i \in]0; 1[$;

5) Вибір елемента з підмножини здійснюється за правилом:

- якщо $0 < y_j < \frac{1}{3}$, обирається x_1 ;
- якщо $\frac{1}{3} < y_j < \frac{2}{3}$, обирається x_2 ;
- якщо $\frac{2}{3} < y_j < 1$, обирається x_3 .

Наприклад, якщо $\frac{1}{3} < y_j < \frac{2}{3}$, то обирається число x_2 . Аналогічно для наступного підмножини $\{x_4, x_5, x_6\}$: якщо $\frac{2}{3} < y_j < 1$, вибирається x_6 ; якщо $0 < y_j < \frac{1}{3}$, тоді – x_7 тощо. Схематичний процес генерації псевдовипадкової послідовності при $z = 3$ наведено на рис. 5.12.

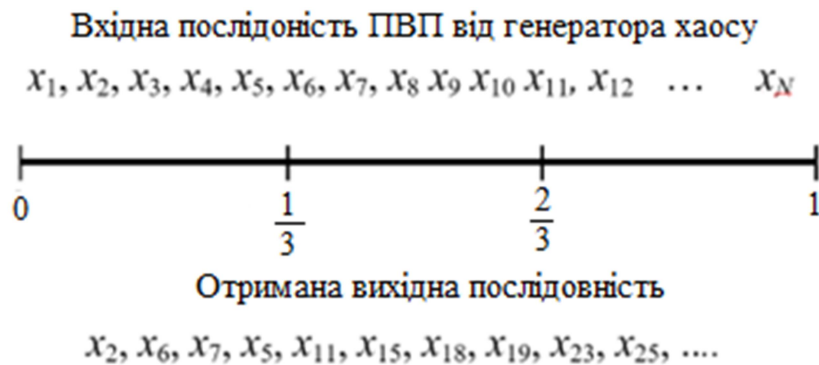


Рисунок 5.12 – Схематичний процес генерації псевдовипадкової послідовності при $z = 3$

У результаті формується послідовність виду:

$$x_\nu, x_{z+\nu}, x_{2z+\nu}, x_{3z+\nu}, \dots; \quad (5.33)$$

де $\nu = 1 \dots z$ - номер обраного елемента в підмножині.

Отримана послідовність (5.33) далі перетворюється у бінарний вигляд за правилами:

$$b_i = \begin{cases} 0, & x_\nu < 0,5, \\ 1, & x_\nu \geq 0,5. \end{cases} \quad (5.34)$$

Вочевидь, що рівень випадковості та криптографічної стійкості отриманих числових послідовностей безпосередньо залежить від кількості елементів z у сформованому підмножині.

Результати проведених досліджень показали, що не всі генератори хаотичних послідовностей у повній мірі задовольняють вимогам системи статистичних тестів NIST. Це свідчить про обмеженість їхнього прямого застосування для формування криптографічно стійких бінарних послідовностей. Зокрема, генератори з логістичним та кубічним відображенням, а також генератор типу «зсув», не пройшли частину тестів на випадковість через вихід значень $P(\chi^2)$ за межі довірчого інтервалу.

Для підвищення якісних характеристик бінарних вибірок запропоновано застосування операції XOR над кількома вихідними послідовностями, згенерованими різними хаотичними генераторами. Експериментальні дослідження показали, що комбінація генератора типу «зсув» та кубічного генератора, які окремо демонстрували незадовільні результати, у поєднанні забезпечила значно кращі статистичні властивості. Це підтверджується тим, що для більшості тестів системи NIST отримані значення $P(\chi^2)$ знаходяться в межах довірчого інтервалу.

Використання кількох хаотичних генераторів одночасно (2–4 і більше) дозволяє суттєво підвищити стабільність статистичних характеристик сформованих бінарних вибірок. Водночас зростає обчислювальна складність, оскільки збільшується кількість операцій, необхідних для формування одного біта. Це слід враховувати при розробці практичних джерел криптографічно стійких послідовностей.

Розроблений алгоритм підвищення криптографічної стійкості генераторів реалізується за рахунок введення додаткової невизначеності у виборі елементів псевдовипадкової послідовності. Використання підмножин із z чисел на всьому інтервалі формування дозволяє підвищити рівень непередбачуваності та стійкості до криптоаналізу. При цьому зі зростанням параметра z криптостійкість алгоритму зростає, однак вимагає більшого обсягу реалізацій

для забезпечення коректної статистичної оцінки. Загалом, результати дослідження підтверджують доцільність комбінування хаотичних генераторів і застосування багаторівневих методів формування послідовностей як ефективного підходу до підвищення криптографічної стійкості інформаційних систем.

5.6.5. Метод формування початкових параметрів для генераторів хаосу

Реалізація динамічного хаосу в системах шифрування потребує розробки методів формування початкових параметрів генераторів на основі введеного користувачем пароля. У більшості відомих досліджень [142, 143] цій проблемі приділено недостатньо уваги, що визначає актуальність роботи та її перспективність у контексті створення нових криптографічних систем на основі хаотичних відображень. Метою дослідження є розробка методу формування початкових параметрів програмних генераторів хаосу шляхом перетворення вхідного пароля за допомогою хеш-функцій.

Розглянемо задачу ініціалізації початкового вектора для одного чи декількох генераторів хаосу, які використовуються для формування гама-послідовності. Очевидно, що початкові стани генераторів мають залишатися секретними. Для цього доцільно застосовувати хеш-функції, які задовольняють криптографічні вимоги: стійкість до відновлення прообразу, а також – до колізій першого та другого роду.

Нехай у системі потокового шифрування [143] використовується один або кілька генераторів хаосу логістичного відображення (5.28), що формують кілька гама-послідовностей. Для підвищення гнучкості алгоритму можуть застосовуватися й інші генератори хаосу. Щоб сформувати початкові параметри (ключі), запропоновано використовувати перетворення символів пароля за допомогою хеш-функції. Це дозволяє відобразити масив символів довільної довжини у бітовий рядок фіксованої довжини (хеш-код). Нехай

пароль має вигляд $\wedge B69PvH * F7UcHv\$3$. Результати його хешування за допомогою різних алгоритмів наведено в табл. 5.2.

Таблиця 5.2 – Результати хешування символів пароля $\wedge B69PvH * F7UcHv\$3$

CRC32	45b8fa89
Naval	3347217c69a19ace3468e10da3a9d585
SHA-1	8fe552437292690894e8f2a23a705413c3e72f24
SHA-256	d8b4966f7267943e74c1a4e1697af81460f8a80448b29785b5cf9c12287c3bde
SHA-384	6a28c21ba8eafe3532c950ff9f3e6894aaef016824991537f883794d80cc1342d63666bcffaa935cc38414203488bd8e
SHA-512	a66d3ea958ba9438956dae1bc6bfe74e624edb0c2034980694575e412f3ab1a4d981027e8ae79eb55f65ffff39bd3e29b5469c73bded51833abd274848b916e3

На основі SHA-512 продемонстровано метод формування початкових параметрів для п'яти послідовностей генератора хаосу (5.28). Важливо зазначити, що значення параметра a суттєво впливає на якість генерованої послідовності, тому його межі вибору обмежені. Для спрощення задачі приймемо $a = 3,9$.

Алгоритм перетворення хеш-коду в початкові параметри генератора хаосу наступний:

- 1) хеш-код розбивається на сегменти певної довжини (наприклад, 3 шістнадцяткові символи);
- 2) кожен сегмент переводиться у десяткове число;
- 3) отримані значення нормуються до інтервалу $y_i =]0; 1[$;
- 4) для покращення статистичних властивостей застосовується перетворення:

$$x_1 = y_1; x_2 = 1 - y_2; x_3 = y_3; x_4 = 1 - y_4; x_5 = 1 - y_5; x_6 = 1 - y_6. \quad (5.35)$$

У табл. 5.3 наведено приклад результатів перетворення для вибраного хеш-коду.

Таблиця 5.3 – Перетворення хеш-коду в початкові параметри генератору хаосу

№ дії	1	2	3	4	5	...	43	M_x
1	a66	d3e	a95	8ba	943	...	e3	
2	2662	3390	2709	2234	2371	...	227	
3	0,2662	0,339	0,2709	0,2234	0,2371	...	0,023	0,237
4	0,2662	0,661	0,2709	0,7766	0,2371	...	0,023	0,481

Як показують результати, отримана послідовність у рядку 3 (табл. 5.3) мала середнє значення $S_x = 0,237$, що значно відхиляється від математичного очікування рівномірного закону $M_x = 0,5$. Застосування додаткового перетворення (5.35) дозволило покращити статистичні властивості: середнє значення зросло до $S_x = 0,481$, що значно ближче до теоретичного.

Отже, запропонований метод формування початкових параметрів генераторів хаосу на основі хешування паролів забезпечує можливість використання різних хеш-функцій для отримання ключових значень. Отриманий хеш-код може бути ефективно перетворений у числові параметри в необхідному діапазоні, що дозволяє підвищити надійність та стійкість криптографічних систем, які базуються на хаотичних відображеннях.

Висновки

У п'ятому розділі дисертації проведено комплексне дослідження параметрів таймерних сигналів та методів їх використання для побудови шумоподібних сигнально-кодових конструкцій у системах захисту інформації:

1 Показано, що варіювання параметрів n , s , i та Δ дозволяє цілеспрямовано керувати спектральними та кореляційними характеристиками сигналів, досягаючи балансу між завадостійкістю, прихованістю та складністю реалізації.

2 Здійснено порівняльний аналіз алгоритмів розширення спектра позиційних і таймерних сигналів, який підтвердив перевагу таймерних конструкцій у забезпеченні підвищеної структурної прихованості.

3 Досліджено вплив вибору розрядності таймерного кодування, кількості значущих моментів модуляції та параметра базового інтервалу на пропускну здатність і рівень структурної прихованості. Встановлено, що збільшення числа можливих реалізацій таймерних сигналів досягається не лише за рахунок розширення алфавіту, але й шляхом комбінування варіантів із різним числом значущих моментів, що дає змогу оптимізувати баланс між складністю та ефективністю.

4. Дана оцінка синтезу псевдовипадкових послідовностей на основі хаотичних відображень. Проведене тестування із застосуванням критеріїв NIST підтвердило, що не всі хаотичні генератори забезпечують належний рівень випадковості, що обґрунтовує необхідність комбінування кількох генераторів і використання операцій XOR для стабілізації статистичних характеристик вибірок. Запропоновані алгоритми синтезу послідовностей із підвищеною криптографічною стійкістю засвідчили ефективність багаторівневого підходу до підвищення непередбачуваності та стійкості до криптоаналізу.

5. Розроблено метод формування початкових параметрів хаотичних генераторів на основі хешування користувацьких паролів. Показано, що таке рішення забезпечує не лише гнучкість у виборі початкових умов, але й підвищує рівень захищеності системи за рахунок стійкості хеш-функцій до колізій і відновлення прообразів.

Загалом, результати досліджень розділу підтверджують доцільність використання таймерних сигналів та хаотичних генераторів у задачах розширення спектра та захисту інформації. Запропоновані підходи дозволяють формувати сигнально-кодові конструкції з високим рівнем завадозахищеності, прихованості та криптографічної стійкості, що створює науково обґрунтовану основу для практичної реалізації сучасних систем безпечного зв'язку.

6 МЕТОДИ ФОРМУВАННЯ ШУМОПОДІБНИХ ТАЙМЕРНИХ СИГНАЛІВ

У розділі представлено підхід до захисту інформації в інформаційно-комунікаційних системах на основі формування шумоподібних таймерних сигналів. Проведено оцінку умов забезпечення енергетичної прихованості для методів розширення спектра за критеріями частотної та енергетичної ефективності використання каналу. Запропоновано використовувати таймерне кодування для синтезу шумоподібних сигналів з адаптивними параметрами, що забезпечують ускладнення їх виявлення засобами радіоелектронної розвідки.

Досліджено вплив параметрів таймерного кодування на складність реалізації, ефективність передачі та стійкість до виявлення. Отримані результати підтверджують перспективність використання шумоподібних таймерних сигналів для побудови багаторівневих систем захисту інформації в умовах дії засобів радіоелектронної боротьби.

6.1. Енергетична прихованість у системах з розширеним спектром

6.1.1. Умови забезпечення енергетичної прихованості та її роль у захисті від засобів радіоелектронної розвідки

В умовах сучасного радіоелектронного протиборства особливої актуальності набуває пошук методів передавання інформації, здатних забезпечувати підвищення завадозахищеності та прихованості функціонування систем зв'язку. Традиційні методи реалізації прихованої передачі, зокрема псевдовипадкова перебудова робочої частоти (ППРЧ) [77, 82], розроблялися переважно для систем, що базуються на позиційних кодах. Подальше зростання показників захищеності цього методу можливе за умови застосування непозиційних кодів, прикладом яких є таймерні сигнали [32].

У низці робіт [77, 82] продемонстровано можливість спільного використання ТСК та ППРЧ, а також запропоновано відповідні алгоритми розширення спектра вузькосмугового сигналу. Проте у зазначених дослідженнях залишилися недостатньо розкритими питання, що стосуються впливу параметрів ТСК на зміну показників завадозахищеності системи зв'язку з ППРЧ. Відомо [1-3], що ключовими характеристиками завадозахищеності є завадостійкість та прихованість, яка може мати енергетичний, структурний, інформаційний та інші аспекти. Енергетична прихованість може бути кількісно охарактеризована через ймовірність виявлення сигналу P_d засобами радіоелектронної розвідки. Для сигналів з розширеним спектром головним чинником, що впливає на величину P_d , є співвідношення сигнал/шум на вході приймача РЕР та база сигналу. Нехай сигнал має енергію E_s , тривалість символу T та займає смугу частот ΔF . База сигналу визначається як:

$$B = \Delta F \times T. \quad (6.1)$$

Ймовірність виявлення сигналу залежить від статистичного критерію прийняття рішення. У випадку узгодженого прийому в умовах адитивної білої гаусової завади (АБГЗ) відношення сигнал/шум на виході кореляційного приймача має вигляд:

$$\text{SNR}_{\text{вих}} = \frac{E_s}{N_0 \times \Delta F}, \quad (6.2)$$

де E_s – енергія сигналу, N_0 – спектральна щільність потужності завад, ΔF – ширина смуги сигналу після розширення спектра.

Енергетична прихованість визначається здатністю сигналу зберігати низький рівень спектральної щільності потужності в порівнянні з фоновим шумом, що ускладнює його виявлення засобами радіоелектронної розвідки

(PER). При цьому ймовірність виявлення сигналу при заданій ймовірності хибної тривоги P_f може бути подана як [43]:

$$P_d = Q(Q^{-1}(P_f) - \sqrt{\text{SNR}_{\text{вих}}}), \quad (6.3)$$

де $Q(x)$ – інтеграл Лапласа, який характеризує функцію помилок; $Q^{-1}(\cdot)$ – обернена функція.

З цього виразу випливає, що збільшення бази сигналу B призводить до зменшення $\text{SNR}_{\text{вих}}$, а отже й до зниження ймовірності виявлення сигналу противником:

$$\lim_{B \rightarrow \infty} P_d \rightarrow P_f. \quad (6.4)$$

Умова (6.3) означає, що сигнал із великою базою складніше виявляються засобами PER. Отже, для забезпечення енергетичної прихованості необхідно, щоб виконується умова:

$$\frac{E_s}{\Delta F} \ll N_0, \quad (6.5)$$

тобто середня потужність сигналу на одиницю смуги значно менша за потужність шуму. Це створює ефект маскування сигналу серед шумового фону. Енергетична прихованість є одним із ключових показників завадозахищеності систем зв'язку, оскільки вона безпосередньо спрямована на ускладнення виявлення факту передавання сигналу засобами радіоелектронної розвідки противника. При цьому сигнал маскується під фонові шуми шляхом розподілу його енергії у широкому діапазоні частот, що призводить до зниження спектральної щільності потужності. Ефективність методів розширення спектра доцільно оцінювати на основі аналізу показників, які складають сукупність умов забезпечення енергетичної прихованості:

1) Перша умова характеризує значення бази сигналу:

$$B = \Delta F \times T \gg 1, \quad (6.6)$$

де T – тривалість бітового елемента.

Велике значення бази сигналу забезпечує низький рівень спектральної щільності потужності, що зменшує ймовірність виявлення сигналу противником.

2) Друга умова характеризує збільшення значення частотної ефективності:

$$\gamma = \frac{R}{\Delta F_{\text{еф}}}, \quad (6.7)$$

де R – швидкість передавання інформації, $\Delta F_{\text{еф}}$ – ефективна смуга займаних частот.

Зі збільшенням смуги сигналу значення γ зменшується, тобто відбувається «погіршення» показника частотної ефективності. Однак це погіршення є необхідною умовою забезпечення енергетичної прихованості, оскільки воно знижує щільність потужності сигналу.

3) Третя умова характеризує ефективність використання каналу за потужністю:

$$\beta = \frac{R}{h_0^2}, \quad (6.8)$$

де h_0^2 – потужність сигналу, розподілена в каналі.

Цей показник відображає ступінь перерозподілу потужності сигналу у широкій смузі частот і безпосередньо пов'язаний із можливістю зменшити рівень сигналу до рівня шуму в каналі. Покращення показника енергетичної ефективності дозволяє вирішувати питання енергетичної прихованості.

6.1.2. Аналіз базових методів розширення спектра

Для завдання аналізу ефективності методів розширення спектра для завдання забезпечення енергетичної прихованості розглянемо три базові методи [2, 76-78, 82]:

- 1) псевдовипадковий перескок робочої частоти;
- 2) пряме розширення спектра псевдовипадковими послідовностями;
- 3) лінійна частотна модуляція.

Усі ці методи задовольняють першій умові ($B \gg 1$) та другій умові, що підтверджує використання розширеної смуги частот. При цьому виконання другої умови супроводжується зменшенням частотної ефективності γ , що є характерною особливістю розширеного спектра. Однак лише метод ПРС-ПВП задовольняє також і третю умову. Це пояснюється суттєвим зменшенням тривалості інформаційного елемента t_0 за рахунок накладення імпульсів псевдовипадкової послідовності з інтервалом $t_{\text{ч}} \ll t_0$. У результаті відбувається ефективний перерозподіл потужності сигналу в широкому діапазоні частот $\Delta F_{\text{эф}}$, що забезпечує мінімізацію значення $\text{SNR}_{\text{вих}}$. Це значно ускладнює виявлення засобами РЕР передаваний сигнал із застосуванням методу ПРС-ПВП. Для методів ППРЧ і ЛЧМ забезпечення енергетичної прихованості можливо лише частково – вони задовольняють першу і другу умови, однак не гарантують достатньої ефективності використання каналу за потужністю. Це обмежує їхні можливості у завданнях прихованого передавання інформації. Ймовірність виявлення P_d залишається відчутно вищою, ніж у випадку ПРС-ПВП, особливо при малих рівнях $\text{SNR}_{\text{вих}}$. Отже, найвищий рівень енергетичної прихованості забезпечує метод ПРС-ПВП, оскільки він задовольняє всі три наведені умови та забезпечує найнижчий рівень P_d . Цей метод є оптимальним для систем, орієнтованих на протидію засобам радіоелектронної розвідки. Методи ППРЧ та ЛЧМ забезпечують лише базовий рівень прихованості, що дозволяє рекомендувати їх для систем, де вимоги до захисту від РЕР є менш жорсткими.

6.2. Методи забезпечення структурної прихованості сигналів на основі псевдовипадкових послідовностей та таймерних сигналів

6.2.1. Особливості використання псевдовипадкових послідовностей розширення спектра

Псевдовипадкові послідовності відіграють важливу роль у системах розширення спектра, забезпечуючи підвищення завадостійкості та певний рівень прихованості передавання інформації. Відомо, що якість ПВП визначається насамперед їхніми кореляційними властивостями, оскільки саме вони визначають здатність сигналів протистояти впливу навмисних і випадкових завад, а також знижувати ймовірність успішного виявлення сигналу засобами радіоелектронної розвідки [9-13]. Фундаментальною характеристикою будь-якої ПВП є її автокореляційна функція (АКФ), яка для ідеальної випадкової послідовності повинна мати вигляд [44]:

$$R_{xx}(\tau) \approx \begin{cases} 1, & \tau = 0, \\ \frac{1}{N}, & \tau \neq 0, \end{cases} \quad (6.9)$$

де N – довжина ПВП, τ – зсув послідовності.

При цьому взаємна кореляційна функція (ВКФ) між різними кодами повинна наближатися до нуля, що мінімізує взаємні завади у системах багатокористувацького доступу. Залежно від методів побудови, у практиці поширені різні типи ПВП. Найпростішими є m -послідовності, які формуються за допомогою лінійних регістрів зсуву. Вони мають хорошу АКФ, проте їхня взаємна кореляція є відносно високою, що обмежує їх використання в багатоканальних системах. Значно кращі властивості демонструють послідовності Голда, які мають обмежені значення ВКФ $(-1, -t, +t-1)$ і забезпечують компроміс між кількістю доступних кодів та рівнем взаємних завад. Ще кращими є послідовності Касамі, особливо «малі», які

характеризуються дуже низькими рівнями ВКФ і тому придатні для задач із підвищеними вимогами до прихованості та завадостійкості. Окреме місце займають послідовності Уолша, що формуються на основі ортогональних матриць Адамара. Їхня головна перевага полягає у строгій ортогональності, яка забезпечує нульову взаємну кореляцію між різними кодами. Це робить їх зручними для багатокористувацьких систем (наприклад, CDMA), проте водночас знижує показник структурної прихованості, оскільки їхня детермінована будова добре відома противнику.

Отже, вибір послідовностей визначається вимогами до системи. Якщо головною метою є підвищення завадостійкості у багатокористувацьких каналах, доцільно використовувати коди Уолша чи Голда. Якщо ж на перший план виходить прихованість і протидія засобам радіоелектронної розвідки, то кращими є послідовності Касамі або хаотичні коди, які мають найбільш непередбачувану структуру.

6.2.2. Оцінка впливу таймерних сигналів на структурну прихованість псевдовипадкових послідовностей Уолша

Послідовності Уолша широко застосовуються у системах із кодовим розділенням каналів завдяки своїй строгій ортогональності [61]. Автокореляційна функція кожного коду має прямокутний характер, а взаємна кореляція між різними кодами дорівнює нулю, тобто:

$$R_{ij}(\tau) = \begin{cases} N, & i = j, \tau = 0, \\ 0, & i \neq j, \end{cases} \quad (6.10)$$

де ij – індекси кодів, N – довжина послідовності.

Ця властивість забезпечує ефективний поділ сигналів у багатокористувацьких системах, проте водночас обмежує їх структурну прихованість. Оскільки коди Уолша формуються на основі матриць Адамара,

їхня побудова є детермінованою і добре відомою противнику. Це створює умови для відносно простого виявлення переданого сигналу засобами радіоелектронної розвідки. Використання таймерних сигналів дозволяє істотно підвищити прихованість системи, навіть при збереженні кодування на основі ПВП Уолша. Ідея полягає в тому, що сигнальна конструкція на інтервалі часу $T_c = m \cdot t_0$ отримує додатковий часовий параметр – зсув або варіацію тривалостей елементів $t_c = t_0 + k\Delta$, що створює ансамбль сигналів зі змінною структурою. Таймерний сигнал, що розширений на основі ПВП Уолша, можна описати як:

$$s(t) = \sum_{k=0}^{N-1} c_k p(t - kT - \Delta_k), \quad (6.11)$$

де $c_k \in \{\pm 1\}$ – елементи коду Уолша, T – тривалість елемента, Δ_k – таймерний зсув, який визначається законом генерації таймерних сигналів, $p(t)$ – елементарний імпульс.

Наявність зсувів $\Delta = t_0/s$ змінює часову структуру послідовності, у результаті чого противник, навіть знаючи базовий код Уолша, стикається з додатковою невизначеністю. Автокореляційна функція сигналу в такому випадку набуває вигляду:

$$R(\tau) = \sum_{k=0}^{N-1} \mathbb{E}[c_k c_{k+\tau}] \varphi(\tau + \Delta_k - \Delta_{k+\tau}), \quad (6.12)$$

де: $\varphi(\cdot)$ – автокореляційна функція елементарного імпульсу.

Отже, завдяки таймерним зсувам відбувається розмиття кореляційних піків, що знижує можливість кореляційного виявлення сигналу. Це безпосередньо підвищує структурну прихованість, оскільки сигнал перестає відповідати класичній «чистій» формі ПВП Уолша. Рівень структурної прихованості можна оцінювати за коефіцієнтом зниження кореляційної видимості:

$$\mu = \frac{R_{max}^{(0)}}{R_{max}^{(\delta)}}, \quad (6.13)$$

де $R_{max}^{(0)}$ – максимальне значення кореляційної функції для ПВП Уолша, $R_{max}^{(\delta)}$ – максимальне значення кореляційної функції після розширення спектра ТСК за допомогою ПВП Уолша.

Чим більшим є коефіцієнт μ , тим вищою є структурна прихованість сигналу. Отже, поєднання ПВП Уолша з таймерними сигналами дозволяє зберегти їхні переваги у вигляді ортогональності, але водночас усунути ключовий недолік – низьку структурну прихованість. Змінювані у часі ансамблі сигналів знижують ефективність методів кореляційного аналізу противника та підвищують рівень захисту інформації в умовах радіоелектронного протиборства.

Нехай c_g – елементи вихідної ПВП, y_g – таймерний сигнал. Процес розширення спектра ТСК має наступний вигляд:

$$w_g = c_g \times y_g, \quad g = 0, 1, \dots, N. \quad (6.14)$$

Періодична автокореляція s_g при зсуві τ дорівнює:

$$R_w(\tau) = \sum_{g=0}^{N-1} w_g w_{g+\tau} = \sum_{g=0}^{N-1} c_g c_{g+\tau} y_g y_{g+\tau}. \quad (6.15)$$

Введемо позначення $z_g(\tau) = y_g y_{g+\tau}$. Тоді

$$R_w(\tau) = \sum_{g=0}^{N-1} c_g c_{g+\tau} z_g(\tau). \quad (6.16)$$

Якщо y_g є випадковою послідовністю ± 1 із малою кореляцією і нульовим середнім, то для $\tau \neq 0$ середнє значення $E[z_g(\tau)]$ близьке до нуля, тому в середньому:

$$E[R_w(\tau)] \approx E[z_g(\tau)]R_c(\tau) \approx 0, \quad (6.17)$$

де $R_c(\tau) = \sum_{g=0}^{N-1} c_g c_{g+\tau}$ – АКФ початкової ПВП. Для $\tau = 0$ маємо $z_g(0) = 1$ і $R_w(0) = R_c(0) = N$. Отже, теоретично маскування діє як скалярний фільтр, що множить кожний член суми АКФ початкового коду на випадкову величину $z_g(\tau)$. У випадку статистичної незалежності y_g від c_g це призводить до ослаблення бічних пелюсток АКФ. Розглянемо таймерний сигнал з наступними параметрами його побудови на інтервалі часу $T_c = m \cdot t_0$, де $m = 4$, $s = 4$, $i = 2$. Для завдання розширення спектра використаємо ПВП Уолша наступної структури на всьому інтервалі ТСК T_c :

$$c_g = \{1 - 1 \quad 1 - 1 \quad 1 - 1 \quad 1 - 1 \quad 1 - 1 \quad 1 - 1 \quad 1 - 1 \quad 1 - 1\}.$$

Таймерний сигнал має наступні тривалості імпульсів:

- 1) $t_{c1} = t_0 + k\Delta = 4\Delta + \Delta = 5\Delta$;
- 2) $t_{c2} = t_0 + k\Delta = 4\Delta + \Delta = 5\Delta$;
- 3) $t_{c3} = t_0 + k\Delta = 4\Delta + 2\Delta = 6\Delta$;

Для даного прикладу обираємо спрощений варіант розширення спектра за умови що:

$$\Delta = \tau \quad (6.18)$$

де τ – елемент імпульсу ПВП Уолша. Це означає, що таймерний сигнал можна представити як послідовність

$$y_g = \{1 \quad 1 \quad 1 \quad 1 \quad 1 - 1 - 1 - 1 - 1 - 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1\}$$

На інтервалі побудови таймерного сигналу кількість значень Δ з урахуванням вибраних параметрів побудови сигнальної конструкції отримуємо: $T_c = m \cdot t_0 = m \times s \times \Delta = 16\Delta$. Кількість елементів розширення з урахуванням (6.19) становить $T_c = 16\tau$. Після розширення спектра ТСК (6.16) отримаємо наступну послідовність:

$$w_g = \{1 - 1 \quad 1 - 1 - 1 \quad - 1 \quad 1 - 1 - 1 \quad 1 \quad 1 - 1 - 1 \quad 1 - 1 \quad 1\}.$$

Коефіцієнт кореляції між ПВП розширення c_g та ТСК y_g становить $K_{cy} = 0,378$. У випадку використання інших послідовностей Уолша для розкриття структури ТСК, наприклад,

$$c_{g+1} = \{1 \ 1 - 1 - 1 - 1 - 1 \ 1 \ 1 \ 1 \ 1 \ -1 - 1 \ -1 - 1 \ 1 \ 1\},$$

коефіцієнт кореляції $K_{c+1,y} = 0,126$. АКФ послідовності Уолша представлена на рис. 6.1. На рис. 6.2 представлений АКФ ТСК після розширення спектра ПВП Уолша. Після перемноження послідовностей Уолша на таймерний сигнал у їхній автокореляційній функції $R_w(\tau)$ відбуваються суттєві якісні зміни. Насамперед спостерігається ослаблення бічних пелюсток: середні значення $R_c(\tau)$ для зсувів $\tau \neq 0$ зменшуються за модулем у порівнянні з вихідною функцією $R_c(\tau)$. Це призводить до зниження кореляційної «видимості» сигналу для стороннього спостерігача. Також відбувається розмиття або навіть знищення періодичності – характерна циклічність з чіткими піками на конкретних τ згладжується, а спектральна картина стає менш регулярною. Бічні компоненти набувають стохастичного характеру: замість великих і детермінованих пелюсток з'являються флуктуації шумоподібного вигляду зі змінним знаком і випадковою величиною. Водночас загальна енергія сигналу не змінюється: значення автокореляції при нульовому зсуві залишається незмінним, тобто $R_w(0) = R_c(0) = N$, але ця енергія розподіляється по іншим лагам більш хаотично.

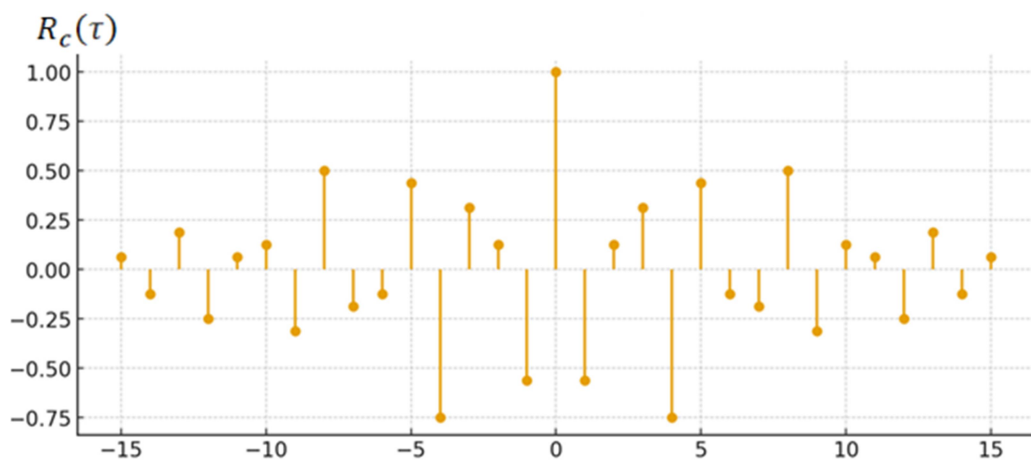


Рисунок 6.1 – АКФ послідовності Уолша

Ефект маскування значною мірою залежить від властивостей ТСК y_g . Якщо сигнальна конструкція має власну циклічність або довготривалу кореляцію, то ефективність приховування зменшується, оскільки в автокореляційній функції $R_w(\tau)$ з'являються нові регулярні компоненти. У такому випадку структура сигналу може бути частково розкрита.

Наслідки для виявлення сигналів полягають у зниженні кореляційного виграшу. Корелятор у приймачі отримує менший пік відгуку $R_w(\tau)$, що фактично зменшує ефективне відношення сигнал/шум (SNR) і веде до падіння ймовірності виявлення P_d при фіксованому рівні хибних тривог P_f .

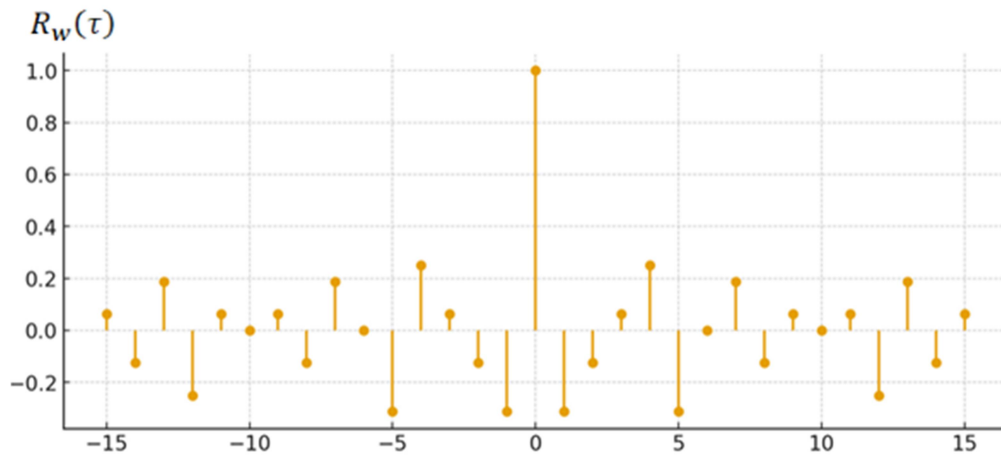


Рисунок 6.2 – АКФ таймерної сигнальної конструкції після розширення спектра ПВП Уолша

При наявності синхронізації між передавачем і приймачем корисний сигнал y_g може бути відновлений, що пояснюється наявністю інформації про структуру ТСК. Для противника, який не володіє інформацією про ТСК, задача виявлення суттєво ускладнюється. Якщо ж таймерний сигнал має низьку ентропію або повторювану структуру, то можливе його відновлення і, відповідно, зниження рівня захисту.

6.3. Вибір бази сигналу для розширення спектра таймерних сигналів

З урахуванням особливостей побудови таймерних сигналів [17, 38, 101, 144] безпосереднє використання алгоритму прямого розширення спектра за допомогою ПВП, який застосовується для позиційних кодів, є неможливим. Це пояснюється тим, що у традиційних системах розширення спектра кожен елемент сигналу має однакову тривалість t_0 , і використовуються при цьому певна база B_{t_0} .

У випадку ТСК тривалість окремих імпульсів може змінюватися та задовольняє умові:

$$t_c \geq t_0. \quad (6.19)$$

Це означає, що необхідно застосовувати інший принцип розширення спектра, адаптований до змінної тривалості імпульсів. Доцільним є виконання розширення спектра не для окремих коротких імпульсів, а на всьому інтервалі формування сигналу T_c . У такому випадку кількість імпульсів ПВП, які використовуються для розширення спектра ТСК, визначається як

$$N_{\tau\text{ТСК}} = B_{t_0} \times m. \quad (6.20)$$

Вочевидь, що значення $N_{\tau\text{ТСК}}$ повинно бути парним деякому числу $N_\Delta = s \times n$, де N_Δ – кількість Δ на інтервалі T_c . Розглянемо приклади узгодження параметрів ТСК з базою B_{t_0} :

1) якщо $s = 4$, $m = 4$, то $N_\Delta = s \times m = 16$, $B_{t_0} = 16$, $N_{\tau\text{ТСК}} = 64$.

2) якщо $s = 4$, $m = 3$, то $N_\Delta = s \times m = 12$, $B_{t_0} = 16$, тоді $N_{\tau\text{ТСК}} = 48$.

У табл. 6.1 показано, що збільшення параметрів s та m призводить до зростання кількості відліків N_Δ , що у свою чергу збільшує необхідну базу

таймерного сигналу $N_{\tau\text{ТСК}}$. Це дозволяє адаптувати систему до різних вимог щодо прихованості, завадостійкості та узгодження з ПВП.

6.4. Синтез шумоподібних сигналів методом прямого розширення спектра таймерних сигнальних конструкцій

Сформуємо широкосмугову послідовність $x_{\text{ТСК}}(T_c, \tau)$ на основі ТСК і ФМ2. Нехай $x(T_c, \Delta)$ бінарний таймерний сигнал на інтервалі його формування $T_c = mt_0$, де $c_{\text{ПВП}}(\tau)$ – послідовність Уолша на інтервалі T_c . При цьому тривалість елементів ПВП $\tau \leq \Delta$. Шляхом перемноження значення рівня кожного i -го розряду послідовності $c_{\text{ПВП}}(\tau)$ на j -те значення рівня таймерного сигналу $x(T_c, \Delta)$ на інтервалі часу T_c отримуємо шумоподібний сигнал:

$$x_{\text{ТСК}}(T_c, \tau) = c_{\text{ПВП}i}(\tau) \times x_{\text{ТСК}j}(T_c, \Delta). \quad (6.21)$$

Таблиця 6.1 – Узгодження параметрів таймерних сигналів при різних значеннях B_{t_0}

№	s	m	$N_{\Delta} = s \times m$	B_{t_0}	$N_{\tau\text{ТСК}}$
1	4	4	16	16	64
2	4	4	16	32	128
3	4	4	16	64	256
4	4	4	16	128	2048
5	8	4	32	16	128
6	8	4	32	32	256
7	8	4	32	64	512
8	8	6	48	16	192
9	8	6	48	32	384
10	8	6	48	64	768

В результаті, кожне позитивне («1») або негативне значення («-1») ТСК замінюється імпульсами ПВП з тривалістю τ . Використання прямої та

інвертованої ПВП $c_{\text{ПВП}}(\tau)$ забезпечує визначення полярності імпульсів тривалістю t_c ТСК при реєструванні ЗМВ на інтервалі T_c при кореляційному прийомі. Далі імпульси $x_{\text{ТСК}}(T_c, \tau)$ надходять на фазовий модулятор, на виході якого утворюється шумоподібний таймерний сигнал:

$$x_{\text{ШТСК фм}}(T_c, \tau) = g(\tau) \cdot \cos(2\pi f_0 \tau + x_{\text{ТСК}}(T_c, \tau)). \quad (6.22)$$

На рис. 6.3 наведено приклад синтезу шумоподібного ТСК $x_{\text{ШТСК фм}}(T_c, \tau)$ з параметрами: $m=4$; $s=4$; $i=2$; $B_{t_0} = 16$, тоді $N_{\text{ТСК}} = 54$. Згідно (3.17) за такими параметрами можна побудувати $N_{\text{ШТСК фм}} = 45$ шумоподібних ТСК. Для РЦК кількість шумоподібних сигнальних комбінацій $N_{\text{рцк фм}} = 16$, що менше в 2,8 рази ніж при використанні ТСК.

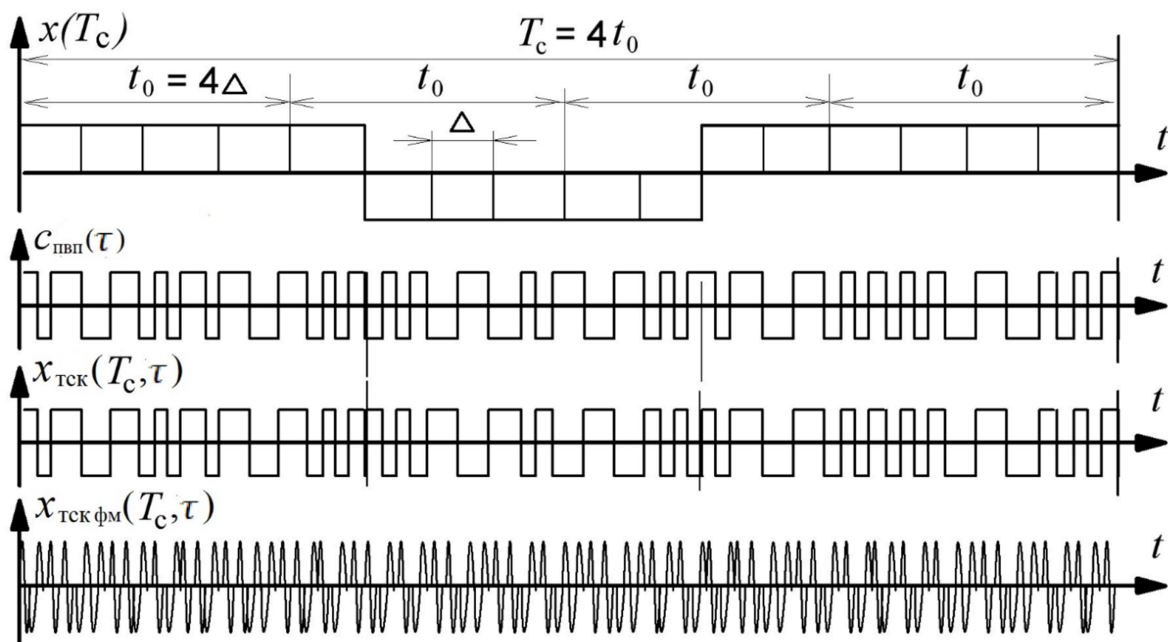


Рисунок 6.3 – Формування шумоподібного таймерного сигналу $x_{\text{ШТСК фм}}(T_c, \tau)$

Такий запас по кількості сигнальних конструкцій дозволяє використати ТСК для формування дозволених комбінацій за допомогою рівняння якості (3.30). Це зменшить кількість реалізацій шумоподібних ТСК, проте дасть

можливість контролювати якість комбінацій, що надходять з каналу в приймач. На кількість реалізацій ТСК впливає значення параметрів s та m . Вибір значення s і m відбувається з урахуванням відношення сигнал/шум h (рис. 5.6), яке визначається перед початком кожного сеансу передачі в результаті тестування каналу.

Отже, адаптація до поточного стану каналу параметрів ТСК при формуванні шумоподібного сигналу дозволяє досягти максимальної пропускної здатності C_m при кожному сеансі передавання інформації.

З урахуванням непозиційності ТСК визначення тривалості імпульсів t_{c1} , t_{c2} і t_{c3} відбувається по точкам екстремумам напруги з виходу інтегратора кореляційного приймача (рис. 6.4) на інтервалі часу T_c . В межах інтервалу $[-\frac{\Delta}{2} \dots \frac{\Delta}{2}]$ визначаються ЗМВ імпульсів ТСК.

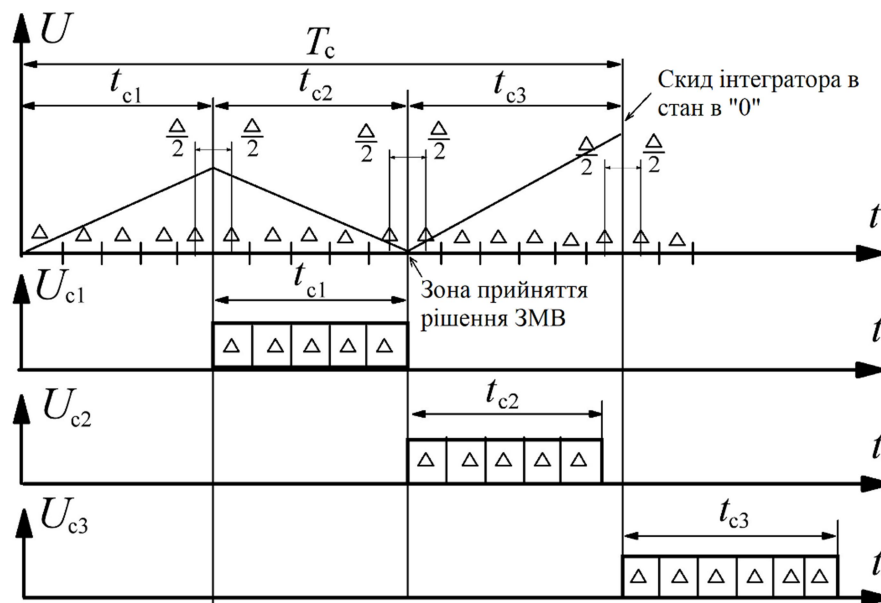


Рисунок 6.4 – Процес визначення ЗМВ імпульсів t_c ТСК з виходу інтегратора кореляційного приймача

6.5. Оцінка структурної прихованості шумоподібних таймерних сигналів

Структурна прихованість шумоподібного таймерного сигналу [141] при розширенні спектра ПВП та використанні певного виду модуляції визначається наступною формулою:

$$S_{\text{ТСК ПВП}} = \log_2 N_p + \log_2 N_{\text{ПВП}} + \log_2 N_{\text{см}}, \quad (6.23)$$

де N_p – кількість реалізацій ТС, $N_{\text{ПВП}}$ – кількість імпульсів ПВП, $N_{\text{см}}$ – кількість сигнальних конструкцій системи модуляції.

На рис. 6.5 надано залежності $S_{\text{ТСК ПВП}}$ від параметрів ТСК і кількості імпульсів розширення ПВП $N_{\text{ПВП}}$. Бачимо, що на загальну прихованість $S_{\text{ТСК ПВП}}$ в більшій мірі впливає показник $N_{\text{ПВП}}$. Наприклад, при параметрах ТСК $m = 8$, $s = 5$, $i = 3$ структурна прихованість $S_{\text{ТСК}} = 12$ дв. вим. При розширенні спектра ПВП $N_{\text{ПВП}} = 64$ та ФМ-2 отримуємо $S_{\text{ТСК ПВП}} = 12 + 64 + 1 = 77$ дв. вим. При цих параметрах шумоподібного сигналу доля $S_{\text{ТСК}}$ і $S_{\text{см}}$ складає усього 18%.

Для збільшення значень $S_{\text{ТСК}}$ і $S_{\text{см}}$ доцільним є використання систем модуляції з більшим числом сигнальних конструкцій (наприклад, КАМ-4 або КАМ-8), а також комбінацій таймерних сигналів з різними ЗММ:

$$N_p(n, i) = \sum_{i=1}^n \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [(n \cdot s) - [(s-1) \cdot i]] - i!}. \quad (6.24)$$

У табл. 6.2 наведені результати розрахунку структурної прихованості шумоподібного таймерного сигналу $S_{\text{ТСК ПВП}}$ у залежності від параметрів таймерної сигнальної конструкції (m , s , i), бази розширення спектра B_{t_0} та застосованого методу модуляції.

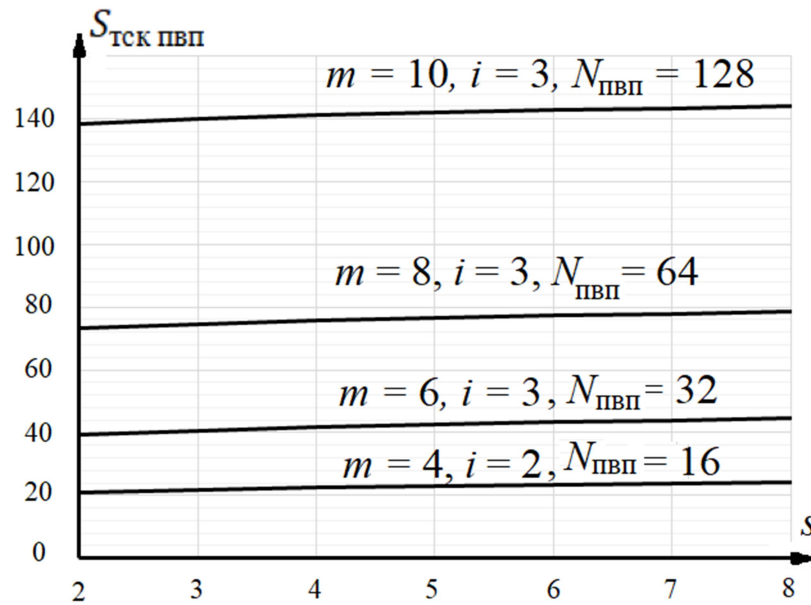


Рисунок 6.5 – Залежності $S_{\text{ТСК ПВП}}$ від параметрів ТСК і кількості імпульсів розширення ПВП $N_{\text{ПВП}}$

З представлених даних видно, що на прихованість сигналу найбільший вплив має база B_{t_0} , яка безпосередньо визначає кількість імпульсів розширення $N_{\text{ПВП}}$. При збільшенні бази від 64 до 256 значення $S_{\text{ТСК ПВП}}$ зростає більш ніж утричі, що демонструє вирішальну роль параметра B_{t_0} у забезпеченні завадостійкості та скритності передачі інформації.

Другим чинником, який суттєво впливає на рівень прихованості, є кількість сигнальних конструкцій системи модуляції $N_{\text{см}}$. При зміні виду модуляції ФМ-2 ($\log_2 N_{\text{см}} = 1$), ФМ-4 ($\log_2 N_{\text{см}} = 2$) та КАМ-8 ($\log_2 N_{\text{см}} = 3$) структурна прихованість збільшується на 2 біти виміру, що підкреслює доцільність використання багаторівневих видів модуляції для підвищення інформаційної безпеки.

Водночас внесок власне таймерної сигнальної конструкції $S_{\text{ТСК}}$ у загальну прихованість є відносно невеликим і визначається кількістю комбінацій, які формуються параметрами m , s , i . Так, при переході від ТСК з параметрами $(m=8, s=5, i=3)$ до $(m=12, s=7, i=5)$ значення $S_{\text{ТСК}}$ збільшується з 12 до 20 дв. вим., однак у загальній структурній прихованості ця різниця складає менше 10%.

Таблиця 6.2 – Структурна прихованість шумоподібного таймерного сигналу

№	Параметри ТСК (m, s, i)	$S_{\text{ТСК}},$ дв.вим.	$B_{t_0}, N_{\text{ПВП}}$	Вид модуляції	$S_{\text{см}},$ дв.вим.	$S_{\text{ТСК ПВП}},$ дв.вим.
1	$m=8, s=5, i=3$	12	64	ФМ-2	1	77
2	$m=8, s=5, i=3$	12	64	ФМ-4	2	78
3	$m=8, s=5, i=3$	12	64	КАМ-8	3	79
4	$m=10, s=6, i=4$	16	128	ФМ-2	1	145
5	$m=10, s=6, i=4$	16	128	ФМ-4	2	146
6	$m=10, s=6, i=4$	16	128	КАМ-8	3	147
7	$m=12, s=7, i=5$	22	256	ФМ-2	1	279
8	$m=12, s=7, i=5$	22	256	ФМ-4	2	280
9	$m=12, s=7, i=5$	22	256	КАМ-8	3	281

Таким чином, для максимізації рівня структурної прихованості доцільно поєднувати три фактори:

- 1) збільшення бази B_{t_0} , що найбільш суттєво підвищує $S_{\text{ТСК ПВП}}$;
- 2) використання багаторівневих систем модуляції (ФМ-4, КАМ-4 та вище);
- 3) оптимальний вибір параметрів ТСК (m, s, i) з урахуванням вимог до швидкодії та складності реалізації.

6.6. Синтез шумоподібного сигналу методом псевдовипадкового перескоку робочої частоти таймерних сигнальних конструкцій

Метод ППРЧ [76, 77, 82] полягає у тому, що робоча частота радіосигналу змінюється за псевдовипадковим законом, відомим лише відправнику і легітимному отримувачу. Це забезпечує високу стійкість сигналу до перехоплення та завад, оскільки сторонній спостерігач без знання ключа не може передбачити частотну послідовність. При використанні методу ППРЧ

робоча частота радіосигналу змінюється за псевдовипадковим законом, який відомий тільки відправнику і отримувачу.

Розширення спектра ТСК відбувається в межах інтервалу T_c шляхом передавання одного або кількох промодульованих елементів Δ таймерного сигналу (ФМ-2 або ФМ-4) на різних частотах. База сигналу визначається наступної формулою:

$$B_f = (F_{max} - F_{min})/\Delta f, \quad (6.25)$$

де F_{max} , F_{min} – межі частотного діапазону; Δf – розмір частотного каналу.

При цьому тривалість сигналу на одній частоті скорочується:

$$t_{\text{пер ппрч}} = \Delta \times z < t_0, \quad (6.26)$$

де $z = 1, 2, \dots, s - 1$ – кількість елементів Δ .

Це дозволяє уникати тривалого перебування сигналу на одній частоті, що ускладнює його виявлення. Розмір частотного каналу Δf пов'язаний з параметром z співвідношенням:

$$\Delta f = 1/\Delta z, \quad (6.27)$$

де $z = 1, 2 \dots sm$. Отже, параметр z визначає, скільки елементів Δ буде передаватися на одній частоті Δf . Зменшення інтервалу часу передавання на одній частоті обґрунтовується особливостями побудови ТСК, а також сучасними можливостями сканерів радіочастотного спектра (SDR), які здатні швидко виявляти та аналізувати сигнали ППРЧ. Чим коротший час перебування сигналу на одній частоті, тим нижчою є ймовірність його ідентифікації та супроводження противником.

Для таймерних сигналів доцільним є використання різних варіантів ППРЧ, які відрізняються швидкістю зміни частоти, кількістю задіяних каналів

та режимом синхронізації. Можна визначити наступні методи ППРЧ: швидкий, повільний, багатоканальний, комбінований.

При повільний ППРЧ кілька елементів Δ передаються на одній частоті перед здійсненням перескоку. Це знижує вимоги до синхронізації та спрощує апаратну реалізацію, оскільки генератор частот працює у більш стабільному режимі. Однак повільний ППРЧ забезпечує меншу прихованість порівняно зі швидким, оскільки сигнал довше залишається на одній частоті й може бути виявлений за допомогою сучасних систем моніторингу спектра. Цей режим доцільно застосовувати в умовах обмежених ресурсів або для систем, де пріоритетом є енергетична ефективність.

При повільний ППРЧ швидкість зміни несучого коливання більша за найквістовий інтервал t_0 у разі, коли використовується позиційне кодування. Для ТСК $\Delta < t_0$, тому час передачі несущого коливання для повільної ППРЧ визначатиметься з урахуванням елемента Δ , тобто:

$$T_{\text{пов ппрч}} = \Delta z, \quad (6.28)$$

де z визначає кількість Δ на інтервалі $T_{\text{пов ппрч}}$.

При виборі інтервалу передавання на одній частоті слід враховувати, що при більшому значенні $T_{\text{пов ппрч}}$ ймовірність ураження радіосигналу завадою в каналі збільшується. Процес розширення спектра ТСК (рис. 6.6 (а)) з параметрами $m = 4$, $s = 4$, $i = 2$ представлений на рис. 6.6 (б) для повільної ППРЧ з $T_{\text{пов ппрч}} = 4\Delta$. Якщо $z = ms$, тоді зміна несущого коливання відбуватиметься на інтервалі $T_{\text{пов ппрч}} = T_c$, тобто для кожної ТСК.

При швидкий ППРЧ робоча частота змінюється після кожного елемента Δ . Це означає, що сигнал не затримується на жодній частоті довше, ніж тривалість одного символу, що робить його максимально прихованим і стійким до виявлення противником. Такий підхід дозволяє ефективно протидіяти сканерам радіочастотного спектра (SDR), оскільки інтервал часу для фіксації

сигналу на одній частоті є мінімальним. Недоліком швидкого ППРЧ є високі вимоги до точності синхронізації між передавачем і приймачем, а також до швидкодії генераторів частот.

При швидкій ППРЧ (рис. 6.6 (в)) інтервал передавання несущого коливання збігається або менше елемента:

$$T_{\text{ш ппрч}} \leq \Delta. \quad (6.29)$$

Можна зазначити, що метод швидкої ППРЧ більш стійкий до завад, оскільки у разі впливу вузькосмугової завади, яка приглушує сигнал у певному підканалі, немає повного спотворення сигнальної конструкції. Таке спотворення призводить до дроблення одного або кількох імпульсів ТСК, що виявляється приймачем. При повільній ППРЧ вплив вузькосмугової завади може призвести до суттєвого спотворення структури ТСК, що ускладнює його відновлення на приймальній стороні. Однак, цей метод більш простий у реалізації, ніж метод швидкої ППРЧ.

Метод багатоканальний ППРЧ полягає у паралельному використанні кількох незалежних частотних каналів, кожен з яких працює за власною псевдовипадковою послідовністю. Це дозволяє значно підвищити пропускну здатність системи, збільшити завадостійкість завдяки просторово-частотному рознесенню та ускладнити задачу противника з виявлення та блокування сигналу. Багатоканальний ППРЧ особливо ефективний у середовищах із сильними навмисними завадами, проте вимагає більш складної архітектури передавача і приймача, а також збільшеного частотного ресурсу.

Комбінований метод ППРЧ поєднує властивості швидкого та багатоканального перескоку, забезпечуючи оптимальний баланс між прихованістю, завадостійкістю та ефективністю використання спектра. Наприклад, частоти можуть змінюватися після кожного елемента Δ , але при цьому використовується кілька паралельних каналів з різними послідовностями перескоку. Такий підхід дозволяє мінімізувати ймовірність виявлення сигналу,

зберігаючи при цьому високу пропускну здатність та адаптивність системи. Основною складністю комбінованого режиму є потреба у складному алгоритмі синхронізації та великій обчислювальній потужності.

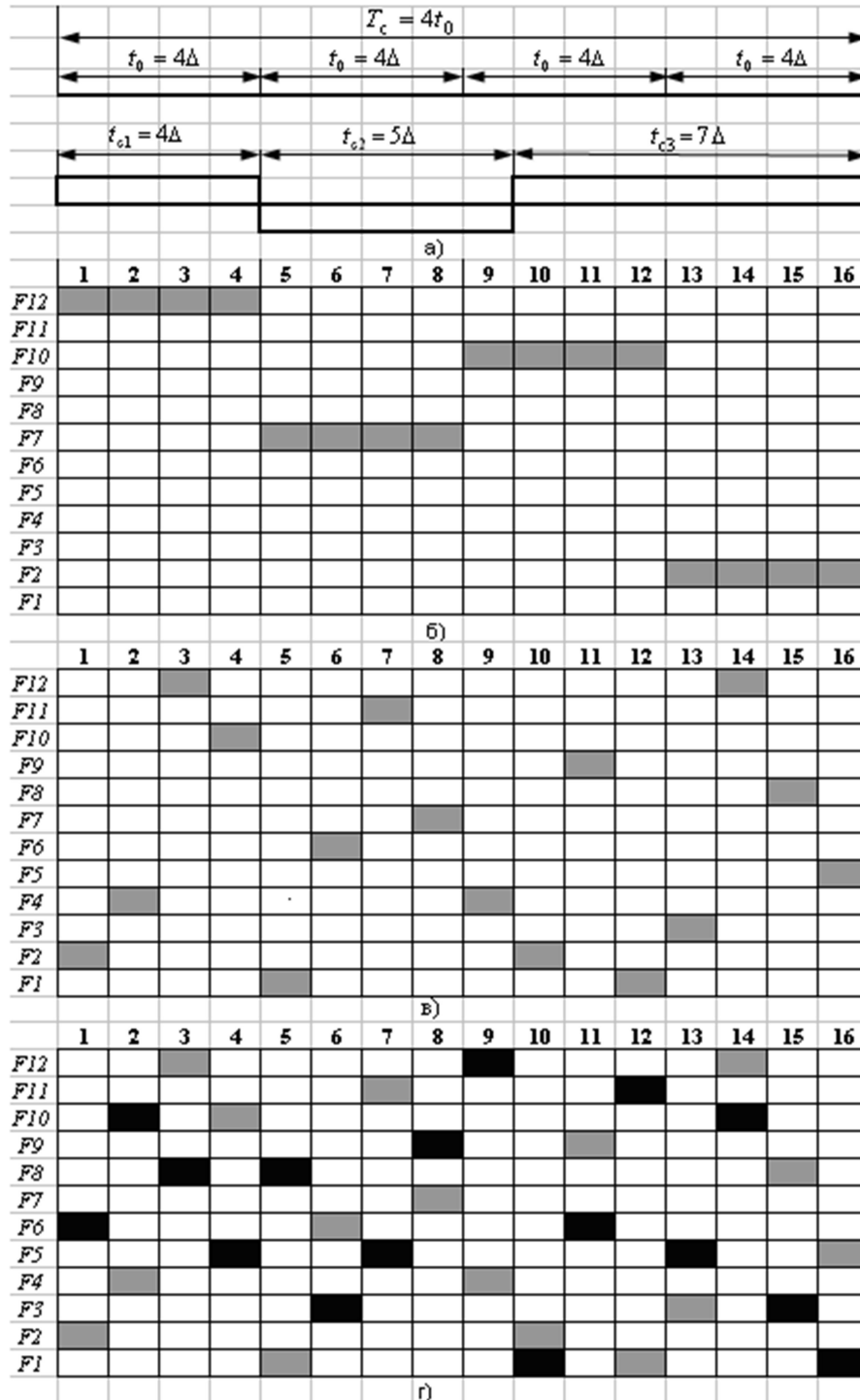


Рисунок 6.6 – Формування шумоподібного ТСК $x_{штск\text{ фм}}(T_c, \tau)$

Іншим варіантом комбінованого методу є поєднання методу прямого розширення спектра за допомогою ПВП та ППРЧ. Цей метод використовує

подвійний механізм розширення спектра та має за рахунок цього два рівня захисту інформації.

На першому рівні спочатку здійснюється пряме розширення спектра (ПРС) шляхом перемноження таймерного сигналу з ПВП довжиною $N_{\text{ПВП ТСК}}$. Це забезпечує шумоподібність сигналу та зменшення спектральної щільності потужності. Автокореляційна функція сигналу набуває властивостей, характерних для шумоподібних процесів: вузький пік при нульовому зсуві та низькі бічні пелюстки. Такий сигнал після розширення спектра можна представити виразом (6.11).

На другому рівні застосовується метод ППРЧ. Кожен блок промодульованих елементів Δ , які вже розширені ПВП, передається на робочій частоті f_i , що вибирається з множини $\{F_{\min}, F_{\min+\Delta f}, \dots, F_{\max}\}$ за псевдовипадковим законом. Сформований сигнал має наступний вигляд:

$$s_i(t) = s(t) \cdot e^{j2\pi f_i t}, f_i \in \mathcal{F}, \quad (6.30)$$

де $\mathcal{F}$ – множина можливих частотних каналів.

Отже, таке комбінування методів забезпечує подвійний захист структури сигналу:

1) пряме розширення спектра за допомогою ПВП приховує структуру таймерного сигналу, розподіляючи його енергію у широкій смузі;

2) використання ППРЧ ускладнює завдання для засобів РЕР, оскільки навіть за умови фіксації спектра на одному з каналів сигнал залишається шумоподібним і важким для синхронізації.

База комбінованого сигналу визначається як добуток базових коефіцієнтів двох методів:

$$B_{\text{комб}} = B_{t_0} \times B_f, \quad (6.31)$$

де B_{t_0} – база ПРС за рахунок ПВП, B_f – база ППРЧ, що визначається шириною частотного діапазону.

Комбінований метод, що поєднує пряме розширення спектра за ПВП та ППРЧ, має низку суттєвих переваг і недоліків. Його основною перевагою є значне ускладнення виявлення сигналу навіть сучасними SDR-сканерами, що робить передачу інформації більш прихованою та захищеною. Крім того, такий підхід підвищує завадостійкість системи у багатопроменевих каналах та в умовах навмисного зашумлення каналу, де традиційні методи розширення спектра можуть бути менш ефективними. Важливою перевагою є також гнучкість налаштування параметрів, яка дозволяє досягати оптимального співвідношення між прихованістю сигналу, пропускну здатністю системи та складністю її реалізації.

Водночас комбінований метод має і певні обмеження. Однією з основних проблем є висока складність синхронізації, оскільки приймач має одночасно відновлювати як псевдовипадкову послідовність, так і послідовність перескоку частот. Це істотно ускладнює апаратну та програмну реалізацію системи. Крім того, застосування такого підходу вимагає значних обчислювальних ресурсів і високої швидкодії апаратури, що може обмежувати його використання в умовах обмежених енергетичних і технічних можливостей.

Таким чином, комбінований метод є перспективним напрямом у побудові систем захищеного зв'язку, але його практична реалізація потребує ретельного балансування між рівнем захищеності та апаратними можливостями системи.

Метод розширення спектра ТСК на основі багатоканальної швидкої ППРЧ представлено на рис. 6.6 (г). Передавання одного елемента Δ на різних піднесучих частотах F_i дозволяє підвищити завадостійкість. Це можливо за рахунок мажоритарного прийняття рішення про полярність елемента Δ за умови використання непарної кількості F_i .

Структурна прихованість шумоподібного ТСК при розширенні спектра методом ППРЧ та використанні певного виду модуляції визначається наступною формулою:

$$S_{\text{тск пвп}} = \log_2 N_p + \log_2 N_{\text{ппрч}} + \log_2 N_{\text{см}}, \quad (6.32)$$

де $N_{\text{ппрч}}$ – кількість можливих варіантів слідування несучих частот.

Розрахунок $N_{\text{ппрч}}$ визначається з урахуванням кількості доступних частот N_f та кількості стрибків в межах інтервалу побудови ТСК $T_c = \Delta \times m \times s$. Для швидкої ППРЧ без повторень несучих частот отримуємо наступну формулу:

$$N_{\text{ппрч бп}} = N_f! / (N_f - ms). \quad (6.33)$$

Збільшити кількість реалізацій можливо з повторенням несучих частот:

$$N_{\text{ппрч п}} = N_f^{ms}. \quad (6.34)$$

Для ТСК (рис. 6.6 (а)) з параметрами $m = 4$, $s = 4$, $N_f = 32$ отримуємо: $N_{\text{ппрч бп}} = 1,26 \times 10^{22}$; $N_{\text{ппрч п}} = 1,21 \times 10^{24}$. Структурна прихованість $S_{\text{тск ппрч бп}} = \log_2 N_{\text{ппрч бп}} = 73,4$ і $S_{\text{тск ппрч п}} = \log_2 N_{\text{ппрч п}} = 80$, що свідчить про переваги методу ППРЧ з повторенням несучих частот приблизно в 1,08 раз.

При комбінованому методі розширення спектра ТСК поєднуються два методи ПРС-ПВП та ППРЧ (рис. 6.7). Спершу спектр ТСК $x_{\text{тск}}(t_c)$ розширюється за допомогою елементів $\tau = \Delta/j$ (де $j = 1, 2, 3, \dots$ – кількість елементів τ на інтервалі Δ) ПВП $x_{\text{тск}j}(T_c, \Delta)$ в широкосмуговий сигнал $x_{\text{тск}}(T_c, \tau) = c_{\text{пвп}i}(\tau) \times x_{\text{тск}j}(T_c, \Delta)$. Після фазового модулятора таймерний сигнал $x_{\text{штск фм}}(T_c, \tau)$ проходить розширення спектра за допомогою методу швидкої ППРЧ:

$$u'(t) = x_{\text{штск фм}}(T_c, \tau) \times U_0 \cos(\omega(g(t)t)), \quad (6.35)$$

де $\cos(\omega(g(t)t))$ – набір частот, який є функцією від кодового сигналу $g(t)$.

Структурна прихованість комбінованого метода оцінюється за формулою:

$$S_{\text{тск пвп-ппрч}} = \log_2 N_p + \log_2 N_{\text{пвп}} + \log_2 N_{\text{см}} + \log_2 N_{\text{ппрч}}, \quad (6.36)$$

де $\log_2 N_{\text{ппрч}} = S_{\text{тск ппрч}}$ – структурна прихованість методу ППРЧ.

Розширення спектра ТСК з параметрами $m = 8$, $s = 5$, $N_{\text{пвп}} = 64$; ФМ-2, $i = 3$, $N_f = 32$ забезпечує структурну прихованість $S_{\text{тск пвп-ппрч}} = 12 + 64 + 1 + 80 = 157$ дв.вим. Бачимо, що використання комбінованого методу розширення спектра ТСК збільшує структурну прихованість у 2 рази та більше в залежності від бази методів ПРС-ПВП та ППРЧ. При інтерпретації структурної прихованості з криптостійкістю можна зробити висновок, що для систем зв'язку з комбінованим розширенням спектра ТСК навіть при невеликих значеннях $N_{\text{пвп}} = 64$ і $N_f = 32$ отримуємо $S_{\text{тск пвп-ппрч}} = 189$ дв. вим., що перевищує криптостійкість системи шифрування DES з довжиною ключа $k_{\text{DE}} = 56$ та AES з $k_{\text{AES}} = 128$.

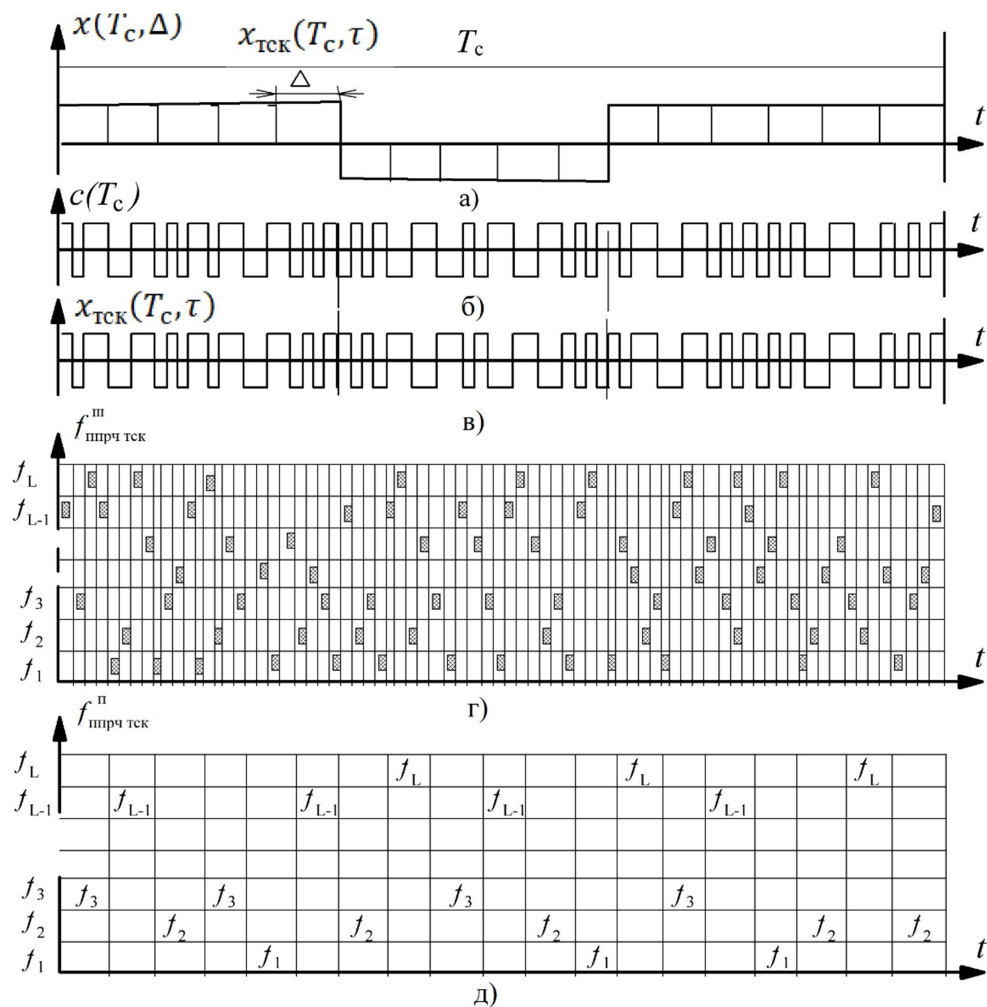


Рисунок 6.7 – Комбіноване розширення спектра ТСК $x_{\text{тск}}(t_c)$

В табл. 6.3. представлені розрахунки структурної прихованості ТСК при різних методах розширення спектра. Проведені розрахунки показують, що рівень структурної прихованості таймерних сигналів суттєво залежить від методу розширення спектра та параметрів системи. Використання класичного ППРЧ без повторів забезпечує мінімальний рівень захисту ($S_{\text{тск ппрч бп}} = 74$), який перевищує криптостійкість DES, але поступається сучасним стандартам. Застосування ППРЧ з повторами дещо підвищує прихованість ($S_{\text{тск ппрч п}} = 81$), однак цей показник залишається нижчим за стійкість AES-128.

Таблиця 6.3 – Розрахунок структурної прихованості ТСК при різних методах розширення спектра

Параметри ТСК, N_f та вид модуляції	Метод розширення спектра	Структурна прихованість методу, дв.вим.	Еквівалентна криптостійкість
$m=4, s=4, i=2,$ $N_f = 32$, ФМ-2	ППРЧ без повторів	$S_{\text{тск ппрч бп}} = 74$	$k_{\text{DES}} = 56$ $< S_{\text{тск ппрч бп}}$
$m=4, s=4, i=2,$ $N_f = 32$, ФМ-4	ППРЧ з повторами	$S_{\text{тск ппрч п}} = 81$	$k_{\text{AES}} = 128$ $> S_{\text{тск ппрч п}}$
$m=8, s=5, i=3,$ $N_{\text{пвп}} = 32,$ $N_f = 32$, ФМ-4	Комбінований ПВП та ППРЧ	$S_{\text{тск пвп-ппрч}} = 126$	$k_{\text{AES}} = 128$ $\approx S_{\text{тск ппрч п}}$
$m=8, s=5, i=3,$ $N_{\text{пвп}} = 64,$ $N_f = 32$, ФМ-4	Комбінований ПВП та ППРЧ	$S_{\text{тск пвп-ппрч}} = 159$	$k_{\text{AES}} = 128$ $< S_{\text{тск пвп ппрч}}$
$m=8, s=5, i=3,$ $N_{\text{пвп}} = 64$ $N_f = 32$, ФМ-4	Комбінований ПВП та ППРЧ	$S_{\text{тск пвп-ппрч}} = 189$	$k_{\text{AES}} = 192$ $\approx S_{\text{тск пвп ппрч}}$
$m=8, s=5, i=3,$ $N_{\text{пвп}} = 128,$ $N_f = 64$, ФМ-4	Комбінований ПВП та ППРЧ	$S_{\text{тск пвп-ппрч}} = 298$	$k_{\text{AES}} = 256$ $\approx S_{\text{тск пвп ппрч}}$

Найбільш ефективним є комбінований метод на основі ПВП та ППРЧ, який демонструє зростання структурної прихованості зі збільшенням довжини ПВП ($N_{\text{ПВП}}$) та кількості частотних позицій (N_f). Зокрема, при $N_{\text{ПВП}} = 32$ забезпечується рівень $S_{\text{ТСК ПВП-ППРЧ}} = 126$, що практично відповідає AES-128, а при $N_{\text{ПВП}} = 64$ і $N_f = 32$ значення досягає $S=159$ та 189 , перевищуючи стандарт AES-128 і наближаючись до AES-192. Подальше збільшення параметрів ($N_{\text{ПВП}} = 128$, $N_f = 64$) дозволяє отримати $S_{\text{ТСК ПВП-ППРЧ}} = 298$, що еквівалентно або навіть перевищує криптостійкість AES-256.

Отже, комбінований метод розширення спектра на основі ПВП та ППРЧ забезпечує максимальний рівень структурної прихованості й може розглядатися як перспективний підхід для побудови високозахисених каналів зв'язку. Його ефективність зростає нелінійно при збільшенні параметрів, що відкриває можливість адаптивної настройки рівня захисту інформації залежно від вимог системи.

6.7. Метод розширення спектра таймерних сигналів з використанням лінійної частотної модуляції

Подальше підвищення ефективності структурної прихованості шумоподібних сигналів досягається шляхом синтезу таймерних сигналів [69] із використанням методу лінійної частотної модуляції (ЛЧМ). Особливість ТСК полягає у можливості формування різних ансамблів сигнально-кодкових конструкцій залежно від початкових параметрів їх побудови. Це забезпечує підвищення структурної прихованості та створює умови для побудови алгоритмів передавання конфіденційної інформації зі змінною структурою шумоподібних сигналів. Отже, актуальним є дослідження властивостей широкосмугових шумоподібних сигналів, синтезованих на основі поєднання ТСК та ЛЧМ, що дозволяє забезпечити як енергетичну, так і структурну прихованість передавання інформації. Метою дослідження є синтез та аналіз ефективності шумоподібних таймерних сигналів на основі ЛЧМ.

ЛЧМ – це метод модуляції, при якому миттєва частота несучого колювання змінюється за лінійним законом протягом тривалості сигналу t_0 . Загальний вигляд ЛЧМ-сигналу можна подати у вигляді:

$$s_{\text{ЛЧМ}}(t) = U_0 \cos(\phi_0 + \phi(t)) = U_0 \cos\left(\phi_0 + 2\pi\left(f_0 t + \frac{b}{2} t^2\right)\right), \quad (6.37)$$

де U_0 – амплітуда сигналу, $f_0 = (F_{\max} + F_{\min})/2$ – центральне значення несучої частоти, $b = (F_{\max} - F_{\min})/T_c$ – апарметр девіації частоти, що характеризує швидкість її зміни, T_c – тривалість сигналу, $F_{\max}$, $F_{\min}$ – межі зміни частоти, ϕ_0 – початкова фаза.

Миттєва частота такого сигналу визначається похідною від фази:

$$f(t) = f_0 + bt, \quad (6.38)$$

що відповідає лінійному закону зміни частоти. Для забезпечення двоїстої модуляції у сигнальних конструкціях використовується пара ЛЧМ-сигналів:

1) зі зростаючою частотою, коли передається значення напруги логічного нуля:

$$S_{\text{ЛЧМ-1}}(t) = U_0 \cos(2\pi f_0 t + \pi b t^2); \quad (6.39)$$

2) зі спадною частотою, коли передається значення напруги логічної одиниці:

$$S_{\text{ЛЧМ-2}}(t) = U_0 \cos(2\pi f_0 t - \pi b t^2). \quad (6.40)$$

У випадку таймерних сигналів дані колювання модулюють імпульси змінної тривалості Δ , що формуються у межах інтервалу T_c . У результаті синтезу формується шумоподібний сигнал:

$$S_{\text{ЛЧМ-ТСК}}(t) = \sum_{k=1}^{s_f} a_k S_{\text{ЛЧМ-}i}(t - k\Delta). \quad (6.41)$$

де $a_k \in \{0, 1\}$ – значення таймерного імпульсу, $S_{\text{ЛЧМ-}i}(t)$ – відповідає одному з опорних ЛЧМ-сигналів (6.39)–(6.40).

Розширення спектра ТСК з використанням ЛЧМ запропоновано на основі двох опорних несучих сигналів $S_{\text{ЛЧМ-1}}(t)$ і $S_{\text{ЛЧМ-2}}(t)$, частоти яких при модуляції імпульсів сигнальної конструкції змінюються за лінійним законом на інтервалі T_c . При цьому використовуються лінійно спадаючий та зростаючий закони зміни частот для $S_{\text{ЛЧМ-1}}(t)$ і $S_{\text{ЛЧМ-2}}(t)$ (рис. 6.8 г) відповідно.

На рис. 6.8 (г) надано процес розширення спектра ТСК $x(T_c, \Delta)$ з параметрами: $m = 4$, $s = 4$, $i = 2$. На рис. 6.9 представлена структурна схема розширення спектра ТСК за допомогою ЛЧМ в передавачі, до складу якого входить:

- 1) перемножувач ($\times$);
- 2) комутатор;
- 3) два генератори Г1 і Г2.

Формування шумоподібного сигналу $S_{\text{ЛЧМ-ТСК}}(t)$ відбувається так: залежно від тривалості імпульсів у межах інтервалу T_c (рис. 6.8 в), комутатор підключає один із генераторів, що формує відповідний опорний сигнал $S_{\text{ЛЧМ-1}}(t)$ або $S_{\text{ЛЧМ-2}}(t)$.

На рис. 6.10 показана структурна схема приймача. Він містить два кореляційні приймачі, які генерують опорні сигнали $S_{\text{ЛЧМ-1}}(t)$ і $S_{\text{ЛЧМ-2}}(t)$. Результати їх перемноження з прийнятим сигналом $S_{\text{ЛЧМ-ТСК}}(t)$ у межах інтервалу T_c надходять на пристрій складання сигналів «+». Далі отриманий сигнал обробляється пристроєм визначення екстремуму (ПВЕ), який фіксує максимальні та мінімальні значення рівня напруги на виході пристрою «+». На цій основі вирішальний пристрій (ВП) виконує відновлення значущих моментів відновлення (ЗМВ), тобто передніх і задніх фронтів таймерного сигналу.

Важливою умовою коректної роботи системи є наявність високоточної тактової та циклової синхронізації. Вона забезпечує відновлення фронтів

імпульсів ТСК з необхідною точністю в межах інтервалу T_c . Неточність синхронізації може призвести до зсуву фазових характеристик ЛЧМ-сигналів та погіршення завадостійкості системи.

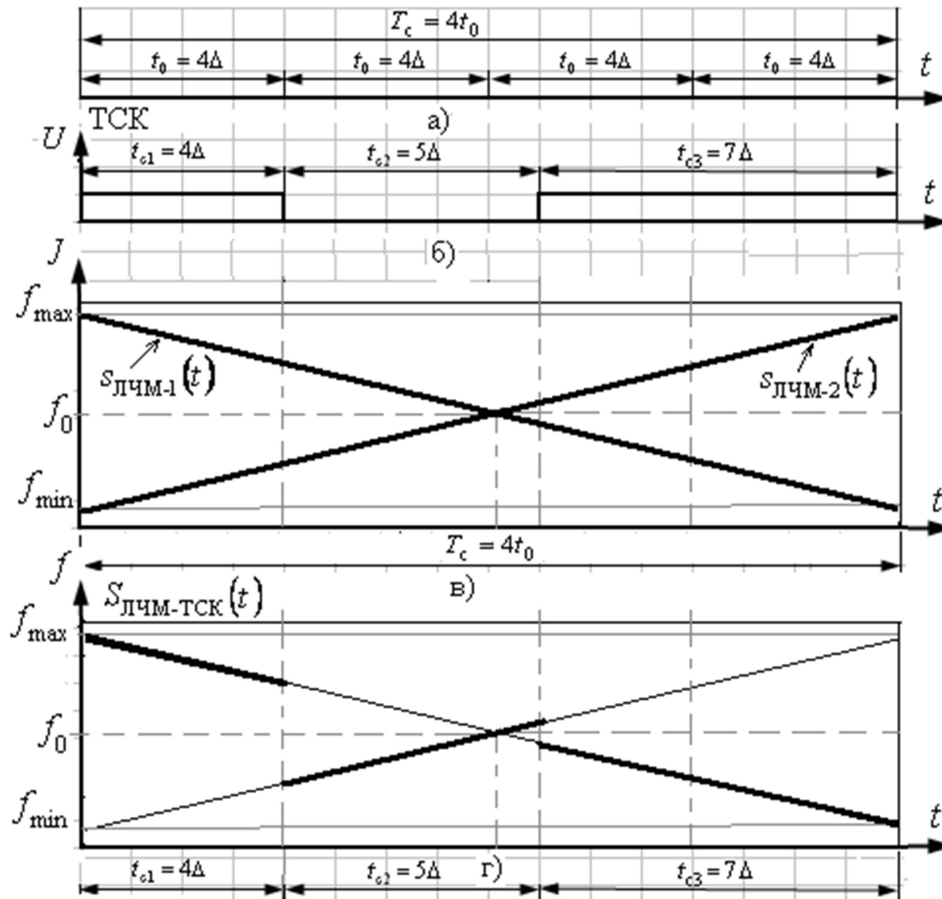


Рисунок 6.8 – Часові діаграми формування широкосмугових ТСК на основі ЛЧМ

Наприкінці кожного інтервалу часу T_c здійснюється обнуління інтеграторів імпульсами циклової синхронізації приймача. Проведено імітаційне моделювання ЛЧМ таймерного сигналу в каналі з шумом [23]. На рис. 6.11 надано часові діаграми відновлення фронтів таймерного сигналу за допомогою двох кореляційних приймачів:

(а) – шумоподібний таймерний сигнал $U_{шпс}$ на вході приймача $h = P_c/P_i = 0,25$;

(б) – результуючий сигнал з виходу пристрою складання сигналів «+»;

(в) – відновлення фронтів ТСК по максимальним та мінімальним значенням напруги сигналу $U_{\text{інт}}$ з виходу ПВЕ.

Результати моделювання дали змогу визначити, що відновлення фронтів сигналу можливо навіть за умови, коли шум набагато більше корисного сигналу.

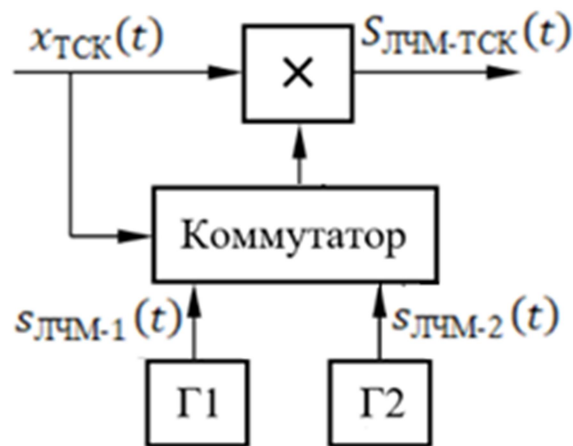


Рисунок 6.9 – Структурна схема розширення спектра ТСК за допомогою ЛЧМ в передавачі

Для перевірки працездатності запропонованого методу було проведено імітаційне моделювання процесу передавання та приймання лінійно-модульованих таймерних сигналів (ЛЧМ-ТСК) у каналі з адитивним білим гаусовим шумом (АБГШ). Метою експерименту є дослідження здатності системи забезпечувати коректне відновлення фронтів таймерного сигналу навіть за умов низького відношення сигнал/шум.

На рис. 6.11 наведено часові діаграми, що ілюструють процес демодуляції та відновлення структури сигналу:

1) (а) – шумоподібний таймерний сигнал на вході приймача при відношенні сигнал/шум:

$$h^2 = \frac{P_c}{P_i} = 0,25,$$

де:

P_c – потужність корисного сигналу;

P_i – потужність завад;

2) (б) – вихід інтегратора кореляційного приймача, що виконує функцію накопичення енергії сигналу протягом інтервалу T_c ;

3) (в) – процес відновлення фронтів таймерної сигнальної конструкції за допомогою детектора пікових значень, що виділяє максимальні та мінімальні екстремуми напруги з виходу інтегратора $\int$.

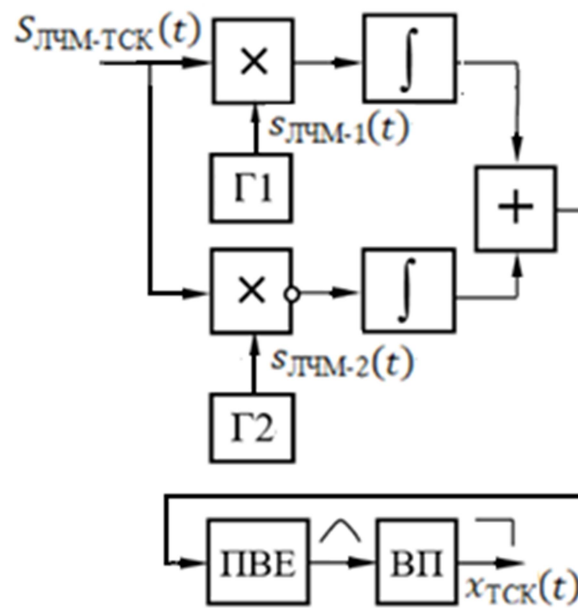


Рисунок 6.10 – Структурна схема виділення імпульсів ТСК з шумоподібного сигналу в приймачі

Аналіз отриманих часових діаграм демонструє, що навіть у випадку, коли потужність шуму перевищує потужність корисного сигналу ($P_i > P_c$), кореляційна обробка дозволяє виділити структуру ТСК завдяки властивостям узгодженої фільтрації. Відновлення фронтів сигналу здійснюється по локальних екстремумах інтегрального відгуку, що підтверджує високу стійкість методу до адитивних завад.

Узагальнено процес можна подати у вигляді:

$$y(t) = \int_0^{T_c} (S_{\text{ЛЧМ-ТСК}}(t) + n(t)) \times S_{\text{оп}}(t) dt, \quad (6.42)$$

де:

$S_{\text{ЛЧМ-ТСК}}(t)$ – переданий ЛМ-ТСК сигнал;

$S_{\text{оп}}(t)$ – опорний сигнал ЛЧМ-генератора (Г1 або Г2);

$n(t)$ – шум АБГШ.

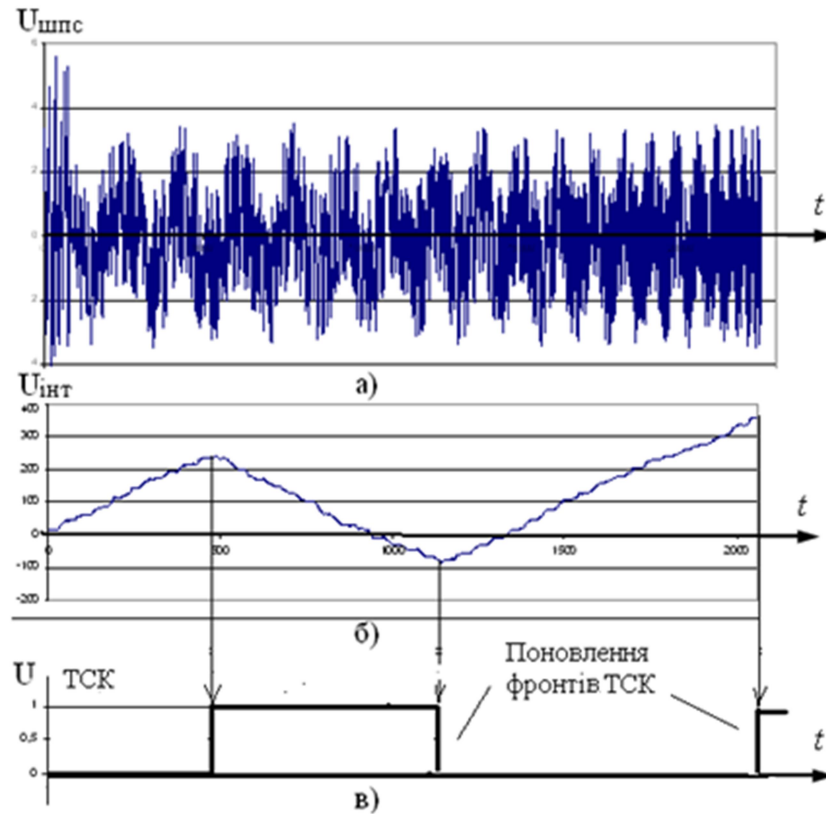


Рис. 6.11. Кореляційний прийом шумоподібного таймерного сигналу

Результати моделювання підтвердили, що застосування ЛЧМ у складі ТСК дозволяє підвищити структурну та енергетичну прихованість сигналу, а також забезпечити надійне відновлення фронтів навіть при критично низькому відношенні сигнал/шум. Це відкриває можливості для використання ЛЧМ-ТСК у системах прихованого та захищеного радіозв'язку, що функціонують в умовах потужних навмисних завад.

6.8. Метод мультиплексування імпульсів таймерних сигнальних конструкцій

В умовах радіоелектронного конфлікту особливе значення набувають питання побудови завадостійких і водночас захищених систем зв'язку. Відомо [79, 80], що завдяки технології OFDM (Orthogonal Frequency Division Multiplexing) забезпечується підвищення завадостійкості в складних умовах поширення сигналу. Дана технологія успішно застосовується як у радіоканалах (наприклад, стандарти IEEE 802.11a та HiperLAN/2), так і у проводових каналах, зокрема в асиметричних цифрових абонентських лініях (ADSL). Разом із тим, не менш актуальним завданням є захист переданої інформації від НСД. Традиційні методи мультиплексування (OFDM, FDM, CDMA) в першу чергу орієнтовані на підвищення пропускної здатності та ефективність використання спектра, але не завжди гарантують прихованість передачі.

До основних переваг технології OFDM слід віднести високу спектральну ефективність, стійкість до радіочастотної інтерференції та низький рівень багатопроменевих спотворень [79, 80]. Це досягається завдяки мультиплексуванню широкосмтових сигналів із ортогональним ущільненням та їх одночасній передачі на різних піднесучих частотах. По суті, OFDM реалізує принцип паралельної багатоканальної передачі, де умови ортогональності піднесучих гарантують мінімальний рівень взаємних завад.

Разом із тим, необхідно зазначити, що дана технологія розроблена для позиційних сигналів, які характеризуються сталою структурою та жорсткою прив'язкою бітів до часових позицій. Це дозволяє легко реалізувати ортогональність у частотній області. Для непозиційних таймерних сигналів, що мають змінну часову структуру та динамічні інтервали кодування, пряме застосування класичного OFDM стає проблематичним. Зокрема, відсутність фіксованої часової позиції ускладнює забезпечення ортогональності каналів та призводить до зниження завадостійкості при традиційному підході.

У зв'язку з цим постає необхідність розробки нового підходу до мультиплексування непозиційних ТСК, який би поєднував переваги багатоканальної

передачі (подібно до OFDM) із властивостями структурної прихованості, притаманними таймерним сигналам. Такий метод дозволить забезпечити одночасну передачу декількох інформаційних потоків із високим рівнем захищеності та стійкості до завад у складних умовах радіоелектронного протиборства.

У системі зв'язку з позиційним кодуванням початкова послідовність елементів тривалості t_0 перетворюється у N паралельних бітових потоків на інтервалі часу:

$$T_c = t_0 N, \quad (6.44)$$

тобто швидкість передавання в кожному каналі зменшується у N разів.

Сформована таким чином бітова послідовність підлягає фазовій або амплітудно-фазовій модуляції (QAM), причому кожен потік передається на власній піднесучій ортогональній частоті $f_1, f_2, \dots, f_N$ [79, 80]. Загальна бітова швидкість передавання при цьому залишається сталою. З метою запобігання порушенню ортогональності, що може виникнути внаслідок ефекту багатопроменевості на вході приймача, вводиться захисний часовий інтервал T_{3I} . Його величина повинна бути не меншою за затримку сигналу $t_{\text{зат}}$ у будь-якому з відбитих променів. У результаті тривалість елементарної послілки зменшується до значення t_0^* , а інтервал передачі дорівнює:

$$T_c = t_0^* N + T_{3I}. \quad (6.45)$$

Розглянемо процес мультиплексування таймерних ТСК. Візьмемо з каналів мультиплексування, кожен з яких формує свій таймерний сигнал $x_i(t)$ з урахуванням стопового інтервалу T_{CTi} . Тоді сумарний мультиплексований сигнал можна записати у вигляді:

$$X_m(t) = \sum_{j=1}^Z x_i(t) \cdot \cos(2\pi f_i t + \varphi_i), \quad (6.46)$$

де

$x_i(t)$ – таймерний імпульс із тривалістю $t_{ci} + T_{CTi}$;

f_i – ортогональна піднесуча частота, що відповідає i -му каналу мультиплексування;
 φ_i – початкова фаза сигналу.

Оскільки імпульси ТСК нееквідистантні, їх подовження за рахунок стопових інтервалів можна записати як:

$$t_{ci}^* = t_{ci} + T_{CTi}, \quad (6.47)$$

Таким чином, для всіх каналів загальний інтервал мультиплексування:

$$T_M = \max_i(t_{ci}) + T_{3I}, \quad (6.48)$$

де T_{3I} – захисний часовий інтервал, що вводиться для компенсації багатопроменевості.

На приймальній стороні процес демультимплексування реалізується шляхом кореляційного виділення фронтів:

$$ZMV_i = \arg \max_i \left\{ \int_0^{T_M} X_M(t) \cdot \cos(2\pi f_i t + \varphi_i) \right\}, \quad (6.49)$$

де ZMV_i – значущий момент відтворення імпульсу для i -го каналу.

Оскільки базовим елементом побудови ТСК є часовий інтервал Δ , а не найквістовий інтервал t_0 , кількість паралельних потоків доцільно визначати з урахуванням кількості імпульсів t_{ci} , що розміщуються в обраному інтервалі часу мультиплексування. На рис. 6.12 (а) наведено процес мультиплексування імпульсів на інтервалі:

$$T_M = zT_c \quad (6.50)$$

де $z = 2$ – кількість каналів мультиплексування для таймерного сигналу з параметрами: $n = 4$; $s = 4$; $i = 2$, зі збільшенням їх тривалості у $L = 2z$ рази.

За заданих параметрів таймерних сигнальних конструкцій (ТСК) на інтервалі часу $T_m = 2t_0n$ формується лише шість потоків мультиплексування, що є меншим, ніж у випадку використання позиційного кодування. Кожен подовжений імпульс t_{ci} має стоповий елемент T_{CTi} змінної тривалості, за допомогою якого забезпечується однаковий інтервал мультиплексування для всіх потоків. При цьому, залежно від полярності імпульсу ТСК, напруга стопового елемента може мати як додатне, так і від'ємне значення. На рис. 6.12 (б) та (в) наведено процес подовження імпульсів таймерних сигналів t_{c1} , t_{c2} , t_{c3} у декілька разів ($L = 4$) при їх мультиплексуванні на інтервалі часу $T_m = 2T_c$. Через нееквідистантність тривалостей імпульсів ($t_{c1}^* = 16\Delta$, $t_{c2}^* = 20\Delta$, $t_{c3}^* = 28\Delta$) відповідні стопові інтервали також матимуть різну довжину. Для імпульсів ТСК-1 (рис. 6.12 (б)) отримаємо: $T_{CT1} = 14\Delta$; $T_{CT2} = 10\Delta$; $T_{CT3} = 2\Delta$, а для імпульсів ТСК-2 (рис. 6.12 (в)): $T_{CT1} = 10\Delta$; $T_{CT2} = 10\Delta$; $T_{CT3} = 6\Delta$. Отже, як видно з рис. 6.12 (б) і (в), захисний інтервал $T_{3I} = 2\Delta$ для всіх каналів мультиплексування залишається однаковим. Очевидно, що збільшення кількості мультиплексованих каналів безпосередньо сприяє підвищенню завадостійкості передавання інформації. Для $z = 2$ та $s = 4$ мультиплексування імпульсів ТСК дало змогу зменшити кількість ортогональних піднесучих частот у порівнянні з технологією OFDM, яка базується на позиційному кодуванні.

Слід підкреслити, що більш складна структура таймерних сигналів порівняно з РЦК, а також принципово інший алгоритм їх мультиплексування, який визначається параметрами n , s , і i , забезпечує підвищення структурної прихованості сигнально-кодових конструкцій (СКК). Це, у свою чергу, ускладнює можливість несанкціонованого доступу до конфіденційної інформації. Фрагмент процесу демультимплексування наведено на рис. 6.13.

Для ТСК-1 показано процедуру виділення фронтів імпульсів із використанням кореляційних приймачів, кількість яких дорівнює числу мультиплексованих каналів. Кожен кореляційний приймач налаштовується на свою опорну частоту f_1 , f_2 , f_3 , яка відповідає каналу мультиплексування на передавальній стороні. Сигнали $U_1(t)$, $U_2(t)$, $U_3(t)$, сформовані на виходах перемножувачів (рис. 6.13 а), надходять до інтеграторів.

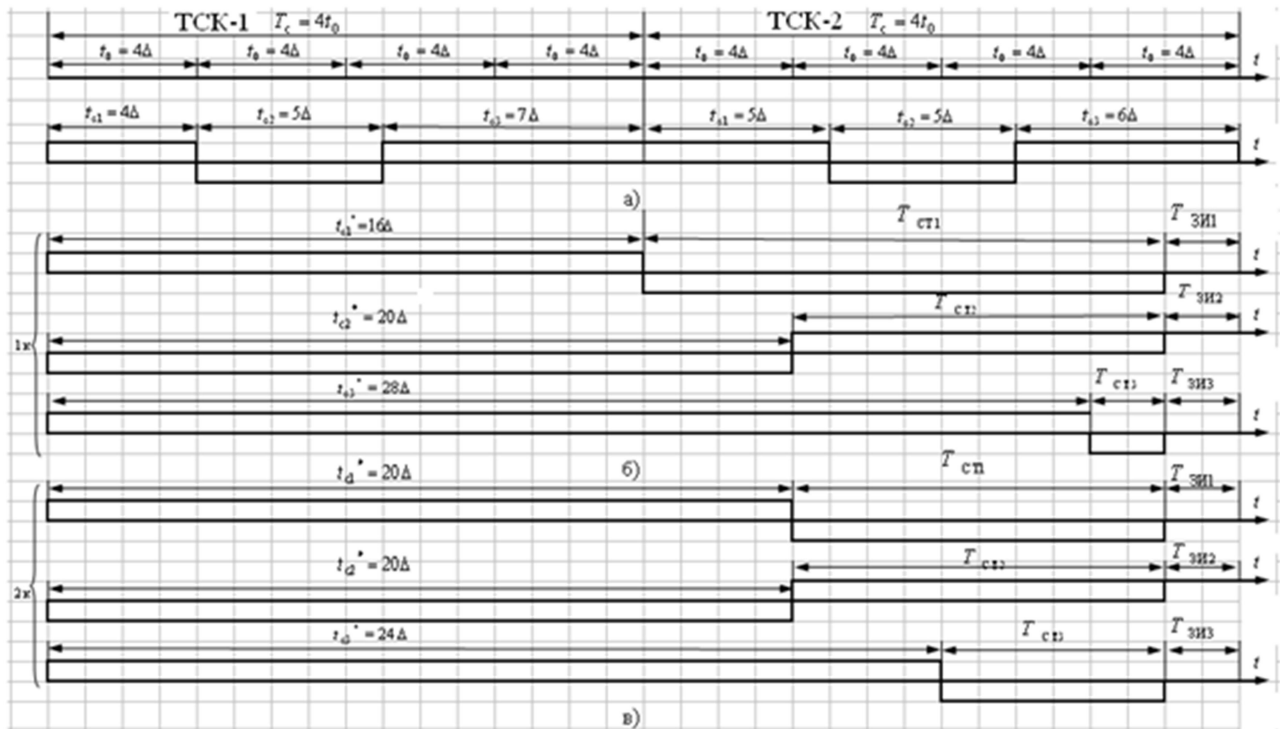


Рисунок 6.12 – Мультиплексування таймерних сигналів $x_{ТСКi}$

За максимальними значеннями напруг $U_{max1}(t)$, $U_{max2}(t)$, $U_{max3}(t)$ (рис. 6.13 б) визначаються ЗМВ таймерних імпульсів (рис. 6.13 в): ЗМВ-1, ЗМВ-2, ЗМВ-3. При цьому помилки реєстрації можливі у випадку відхилення ЗМВ від істинних значень $t_{c1}^* = 16\Delta$, $t_{c2}^* = 28\Delta$, $t_{c3}^* = 20\Delta$ хоча б на величину $\pm\Delta$. Завдяки незалежному рознесенню за часом та параметрами побудови ТСК, забезпечується квазіортогональність каналів, що дає змогу одночасно передавати декілька інформаційних потоків без значного зростання взаємних перешкод.

Основні переваги запропонованого методу полягає в наступному:

- 1) формування багатоканальної структури сигналу без втрати шумоподібних властивостей;
- 2) підвищення структурної прихованості завдяки змінності параметрів таймерного кодування;
- 3) стійкість до багатопроменевого поширення та активних завад;
- 4) можливість інтеграції з криптографічними методами захисту.

Отже, мультиплексування імпульсів ТСК можна розглядати як перспективний напрям розвитку захищених широкосмугових систем зв'язку, що поєднують

властивості OFDM та таймерних сигналів, але з вищим рівнем прихованості інформації.

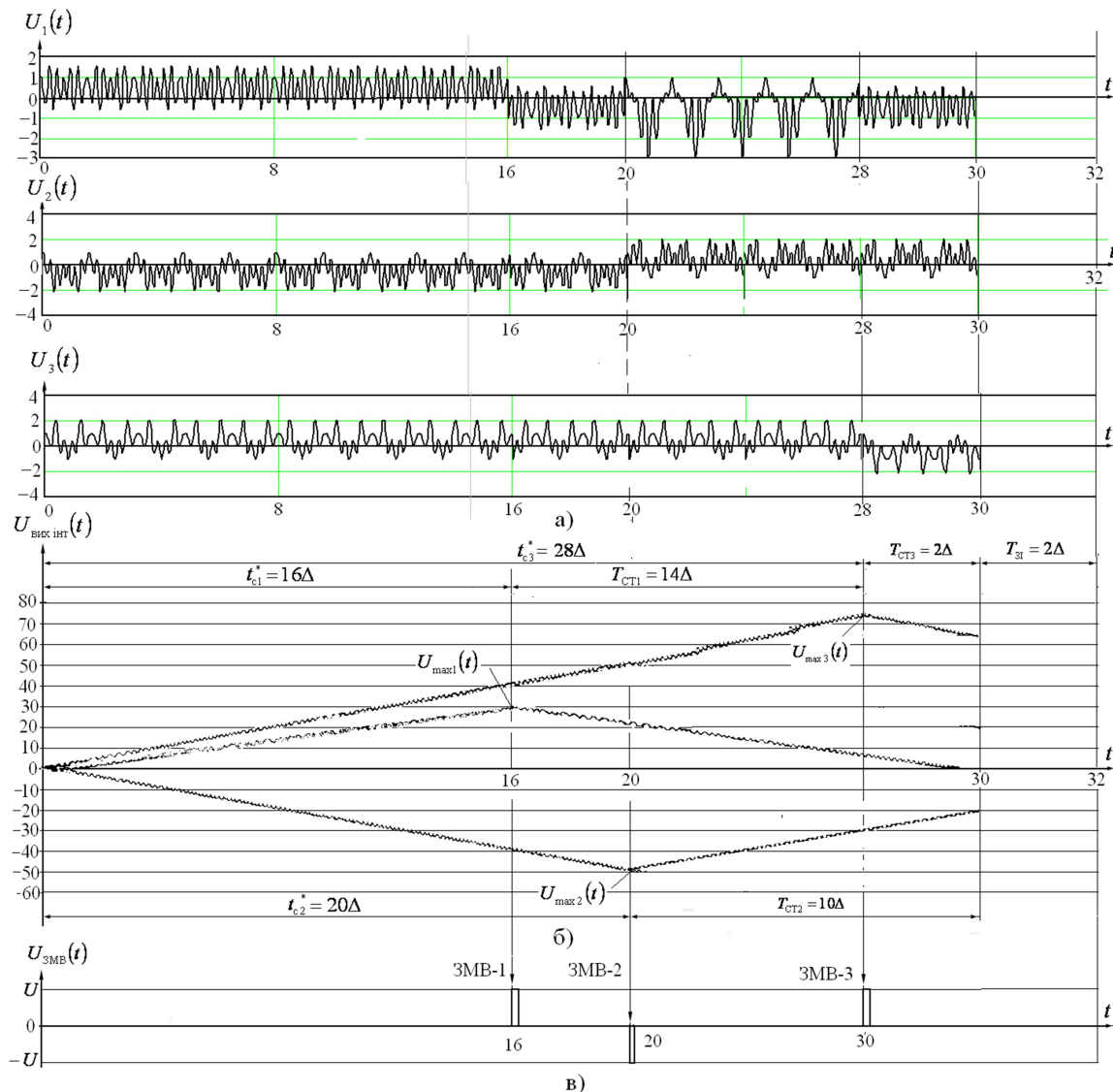


Рисунок 6.13 – Процес виділення фронтів імпульсів ТСК-1 за допомогою кореляційних приймачів

6.9. Метод розширення спектра таймерних сигналів на основі хаотичних коливань

Підвищення рівня структурної прихованості сигнально-кодових конструкцій може бути досягнуте шляхом розширення ансамблю використовуваних сигналів за рахунок застосування реалізацій хаотичних процесів [132, 146-148]. Це обґрунтовує актуальність дослідження методів формування сигнальних конструкцій на основі інтеграції широкосмугових

хаотичних сигналів та таймерних сигналів [96, 106, 115]. У сучасних алгоритмах передавання [115, 152], що ґрунтуються на хаотичних динамічних системах, можна виділити декілька ключових підходів до модуляції:

1) Хаотичне маскування, при якому інформаційний сигнал $x(t)$ підсумовується з хаотичним сигналом $c(t)$, після чого комбінований сигнал передається каналом зв'язку:

$$s(t) = x(t) + c(t). \quad (6.51)$$

2) Перемикання хаотичних режимів реалізується наступним чином: у випадку бінарної інформаційної послідовності «1» кодується однією реалізацією хаотичного сигналу, а «0» – іншою. Такий підхід забезпечує прихованість і ускладнює несанкціоноване відновлення інформації.

Для побудови багаторівневої кодової послідовності використовується одна з реалізацій хаотичного сигналу $c(t)$, яка проходить процедури дискретизації (відповідно до теореми відліків) і квантування за рівнем. У результаті формується дискретна послідовність c_n , яка розбивається на сегменти довжиною T_c , що відповідає тривалості таймерних сигналів. Саме ці сегменти надалі застосовуються у процесі синтезу СКК [66].

Нехай на інтервалі $T_c = nt_0$ формується бінарний таймерний сигнал $x(T_c)$, а багаторівнева хаотична послідовність $c(T_c)$ описується розрядами c_i , кожен з яких відповідає певному рівню. Оскільки тривалість розрядів хаотичної послідовності є меншою за Δ таймерного сигналу, синтез вихідної сигнально-кової конструкції здійснюється за принципом:

$$x_{\text{СКК}}(T_c) = c_i(T_c) \times x_j(T_c), \quad (6.52)$$

де

$c_i(T_c)$ – значення рівня хаотичної послідовності на даному інтервалі;

$x_j(T_c)$ – відповідний рівень бінарного таймерного сигналу.

Таким чином, кожна позитивна полярність («1») таймерного сигналу замінюється фрагментом прямої хаотичної послідовності, а негативна («-1») – відрізком тієї ж послідовності, але інвертованої за рівнями. Такий підхід дозволяє не лише передавати інформацію про полярність таймерного сигналу, але й забезпечує можливість кореляційного виділення моментів зміни фронтів у межах інтервалу T_c . На рис. 6.14 подано структурну схему формування вихідного сигналу в передатчику такої системи зв'язку.

Припустимо, що система є лінійною, а синхронізація в каналі зв'язку – ідеальною. У такому випадку розглянемо процес кореляційного приймання сигналу (рис. 6.15). Нехай $x_{\text{сск}}'(T_c)$ – сигнал на вході приймача. Для його обробки кожен розряд прийнятого сигналу множиться на відповідний розряд початкової прямої хаотичної послідовності, відомої приймачу [69]:

$$y(T_c) = x_{i \text{ сск}}'(T_c) \times c_i(T_c). \quad (6.53)$$

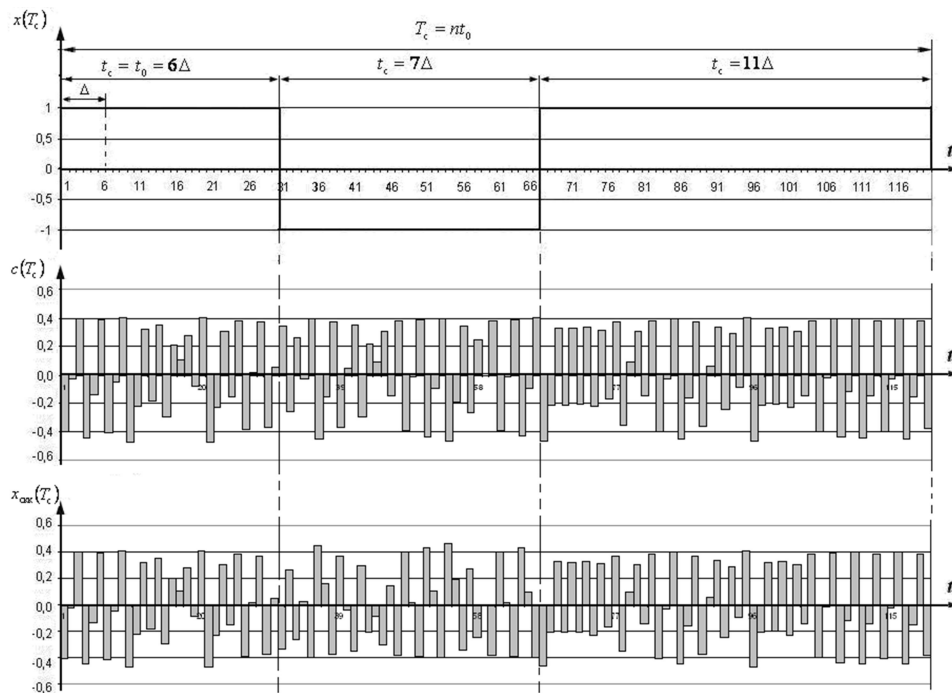


Рисунок 6.14 – Процес розширення ТСК хаотичними багаторівневими послідовностями

Отримані результати множення, з урахуванням амплітуди та полярності, накопичуються інтегратором протягом одного періоду хаотичної послідовності T_c . Далі вирішальний пристрій аналізує рівень напруги на виході інтегратора $U_{\text{інт}}$ і за його максимальним або мінімальним значенням визначає момент та знак зміни полярності таймерного сигналу. Після цього інтегратор обнуляється, а вирішальний пристрій формує відновлений таймерний сигнал із затримкою на один тактовий інтервал T_c .

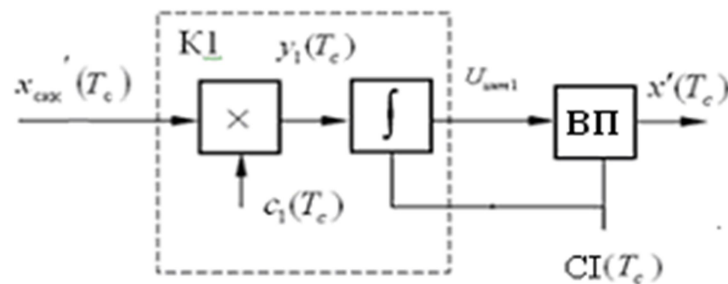


Рисунок 6.15 – Виділення переходів широкосмугової ТСК за допомогою кореляційного приймача на інтервалі часу $T_c = nt_0$

На рис. 6.16 подані часові діаграми процесу кореляційного приймання. У цьому випадку структурна прихованість сигнально-кодових конструкцій визначається співвідношенням:

$$S = S_{\text{ТСК}} \times S_{\text{ХСК}}. \quad (6.54)$$

Таким чином, використовуючи різні способи формування ТСК відповідно до (6.54), можна оцінювати структурну прихованість синтезованих СКК з урахуванням кількості рівнів розширювальної псевдовипадкової послідовності на основі реалізацій динамічного хаосу [153]. Варіюючи параметрами n , s і i для ТСК та d для хаотичної сигнальної конструкції (ХСК), забезпечується формування сигнальних конструкцій із наперед заданим рівнем структурної прихованості.

Подальше вдосконалення цього методу можливе шляхом застосування розширювальних послідовностей з двома сигнатурами [67]. Для побудови сигнальної конструкції на основі ТСК і хаотичних сигналів на передавальній стороні протягом інтервалу T_c обираються дві взаємно ортогональні реалізації хаотичного сигналу c_1 та c_2 (рис. 6.17). На їх основі формуються багаторівневі кодові послідовності $c_1(T_c)$ і $c_2(T_c)$, що проходять дискретизацію за часом (відповідно до теореми відліків) і квантування за рівнем [61, 67]. Ці послідовності використовуються при побудові сигнально-кодових конструкцій. У процесі дослідження експериментально були відібрані слабкорельовані послідовності $c_1(T_c)$ і $c_2(T_c)$, для яких коефіцієнт кореляції становив $2,039 \times 10^{-4}$.

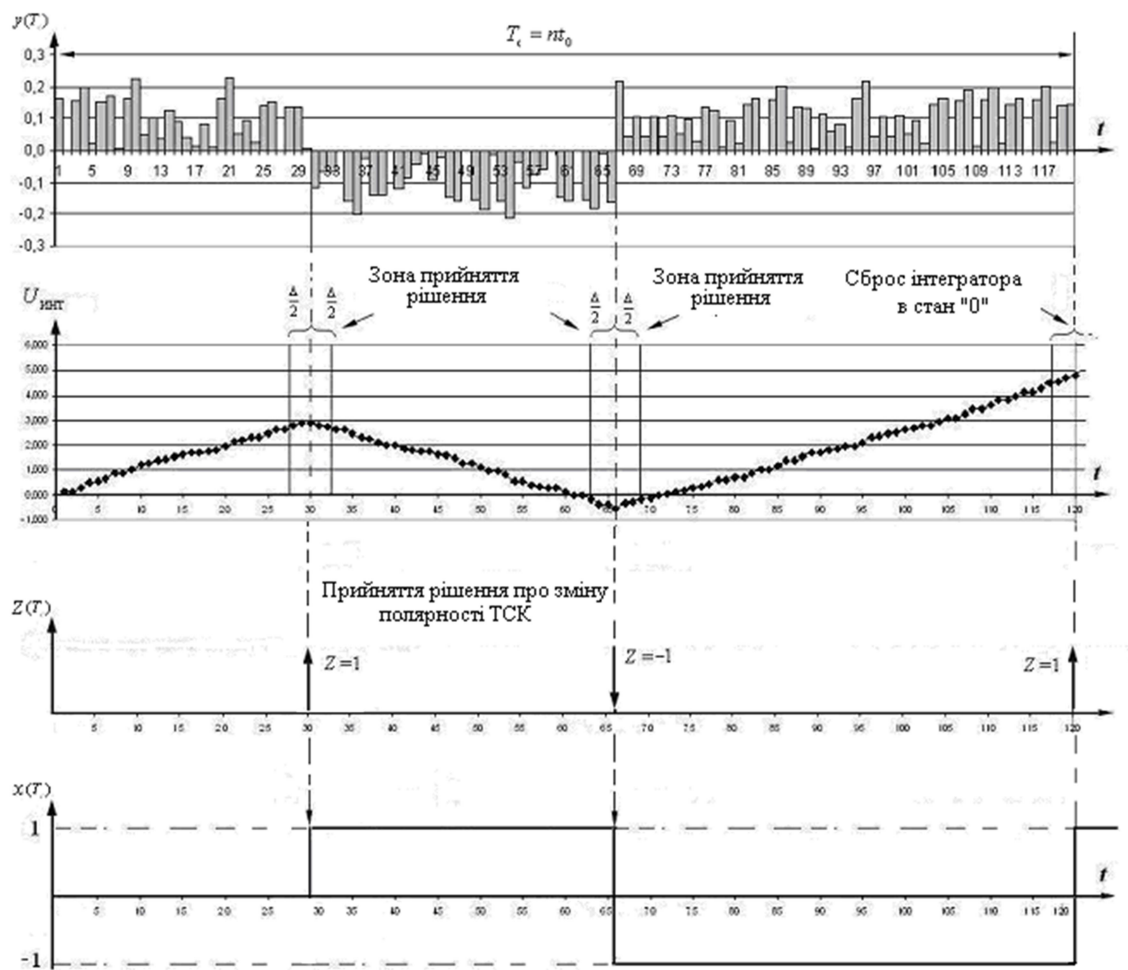


Рисунок 6.16 – Часові діаграми кореляційного приймання широкопasmового сигналу на інтервалі $T_c = nt_0$

Нехай $x(T_c)$ – бінарний таймерний сигнал на інтервалі його формування $T_c = nt_0$, а $c_1(T_c)$ і $c_2(T_c)$ – багаторівневі кодові послідовності на тому ж часовому інтервалі T_c . При цьому тривалість розрядів хаотичної послідовності є меншою за Δ таймерного сигналу. Синтез СКК $x_{\text{СКК}}(T_c)$ на інтервалі T_c здійснюється шляхом множення значень розрядів хаотичної послідовності $c_1(T_c)$ на позитивні рівні таймерного сигналу $x_j(> 0; T_c)$. Якщо ж таймерний сигнал має негативний рівень $x_j(< 0; T_c)$, то його модуль множиться на розряди послідовності $c_2(T_c)$. Таким чином, кожна позитивна полярність («1») у бінарному таймерному сигналі замінюється вибіркою сигналів із послідовності $c_1(T_c)$, тоді як негативна полярність («-1») відтворюється за рахунок використання відповідних відліків із послідовності $c_2(T_c)$. Застосування двох хаотичних послідовностей $c_1(T_c)$ і $c_2(T_c)$ не лише дозволяє коректно відображати полярність таймерного сигналу, але й забезпечує можливість реєстрації моментів зміни його фронтів на інтервалі T_c під час кореляційного приймання:

$$x_{\text{СКК}}(T_c) = c_{1i}(T_c) \times x_j(> 0; T_c) + c_{2i}(T_c) \times |x_j(< 0; T_c)|. \quad (6.55)$$

Часові діаграми формування вихідного сигналу $x_{\text{СКК}}(T_c)$ на передавальній стороні системи конфіденційного зв'язку наведені на рис. 6.17.

Припустимо, що система є лінійною та в каналі забезпечена ідеальна синхронізація. Тоді процес кореляційного приймання сигналу (рис. 6.18) можна описати наступним чином. Нехай $x'_{\text{СКК}}(T_c)$ – сигнал на вході приймача. Кожен розряд прийнятого сигналу $x'_{\text{СКК}}(T_c)$ множиться на відповідний розряд опорних послідовностей $c_1(T_c)$ та $c_2(T_c)$:

$$y_1(T_c) = x'_{i \text{ СКК}}(T_c) \times c_{1i}(T_c) \quad (6.56)$$

$$y_2(T_c) = x'_{i \text{ СКК}}(T_c) \times c_{2i}(T_c). \quad (6.57)$$

Отримані сигнали $y_1(T_c)$ і $y_2(T_c)$, з урахуванням їх амплітуди та полярності, інтегруються у двох незалежних накопичувачах протягом одного періоду хаотичної послідовності T_c . Далі значення вихідних напруг $U_{\text{інт1}}$ та $U_{\text{інт2}}$ подаються на підсумовуючий пристрій, де виконується їх складання та фіксація.

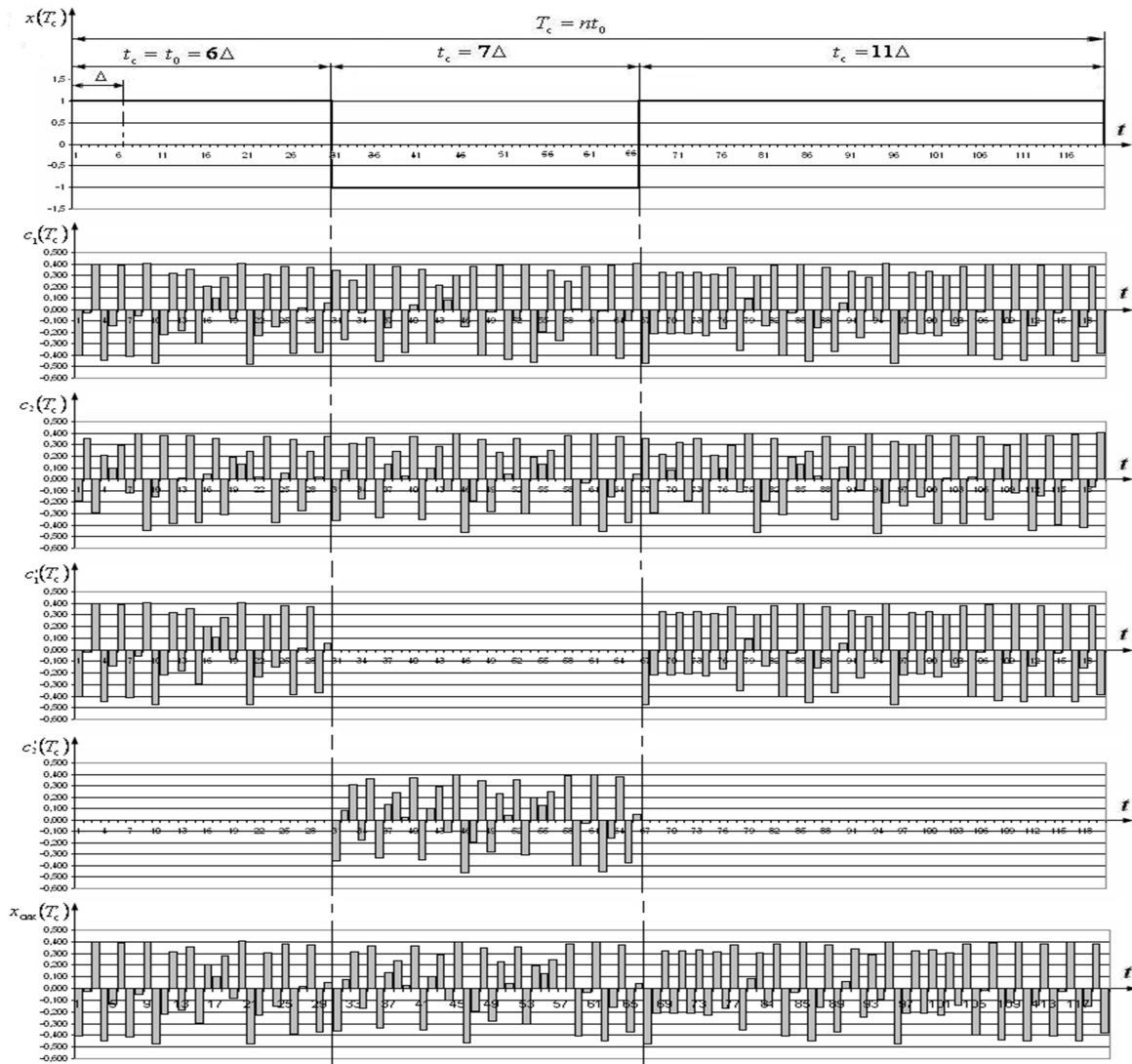


Рисунок 6.17 – Синтез вихідного сигналу $x_{\text{сск}}(T_c)$ на основі ТСК і двох опорних сигнатур $c_1(T_c)$ і $c_2(T_c)$

Для ухвалення рішення про полярність прийнятого імпульсу ТСК вирішальний пристрій аналізує рівні інтегральних напруг $U_{\text{інт}}^*$ у межах часового інтервалу T_c . За їх максимальним або мінімальним значенням визначається знак z та момент зміни полярності таймерного сигналу. Після цього вирішальний

пристрій формує відновлену реалізацію таймерного сигналу із затримкою на один тактовий інтервал T_c , а інтегратор переводиться у початковий (нульовий) стан:

$$x_{\text{срк}}'(T_c) = \max \left[\int_0^{T_c} (y_1(T_c) + y_2(T_c)) dt \right]. \quad (6.58)$$

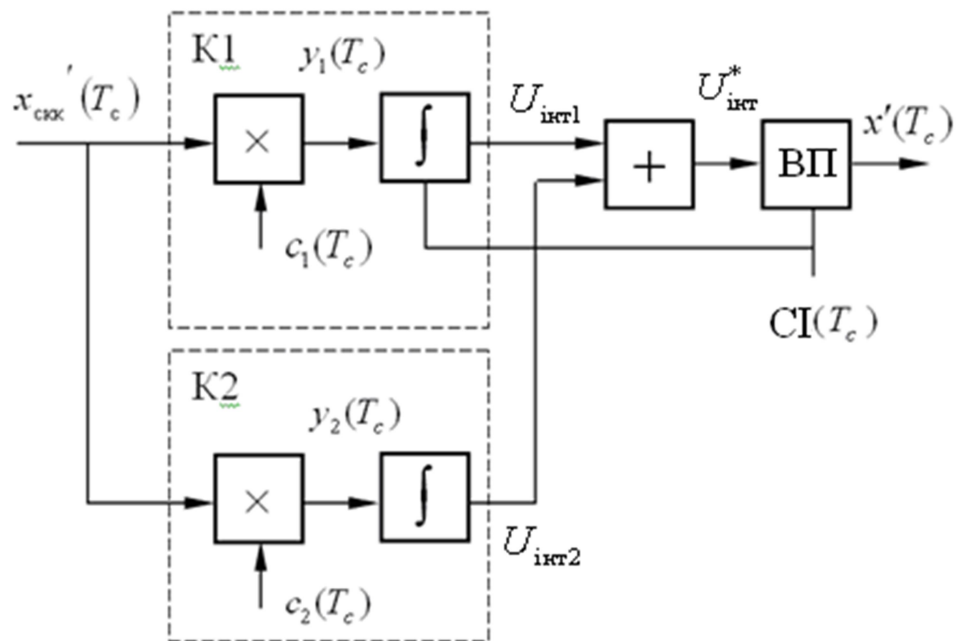


Рисунок 6.18 – Структурна схема кореляційного приймача широкосмугового таймерного сигналу

На рис. 6.19 подано часові діаграми процесу кореляційного приймання сигналу. Аналіз показує, що використання двох кореляторів із відповідними опорними сигнатурами $c_1(T_c)$ і $c_2(T_c)$ забезпечує можливість реєстрації ЗМВ імпульсів ТСК. Разом з тим, на точність ухвалення рішення щодо ЗМВ значно впливають властивості хаотичних послідовностей $c_1(T_c)$ та $c_2(T_c)$. Їхня ортогональність повинна забезпечуватися не лише в межах одного інтервалу T_c , а й на проміжках τ_c між окремими вибірками.

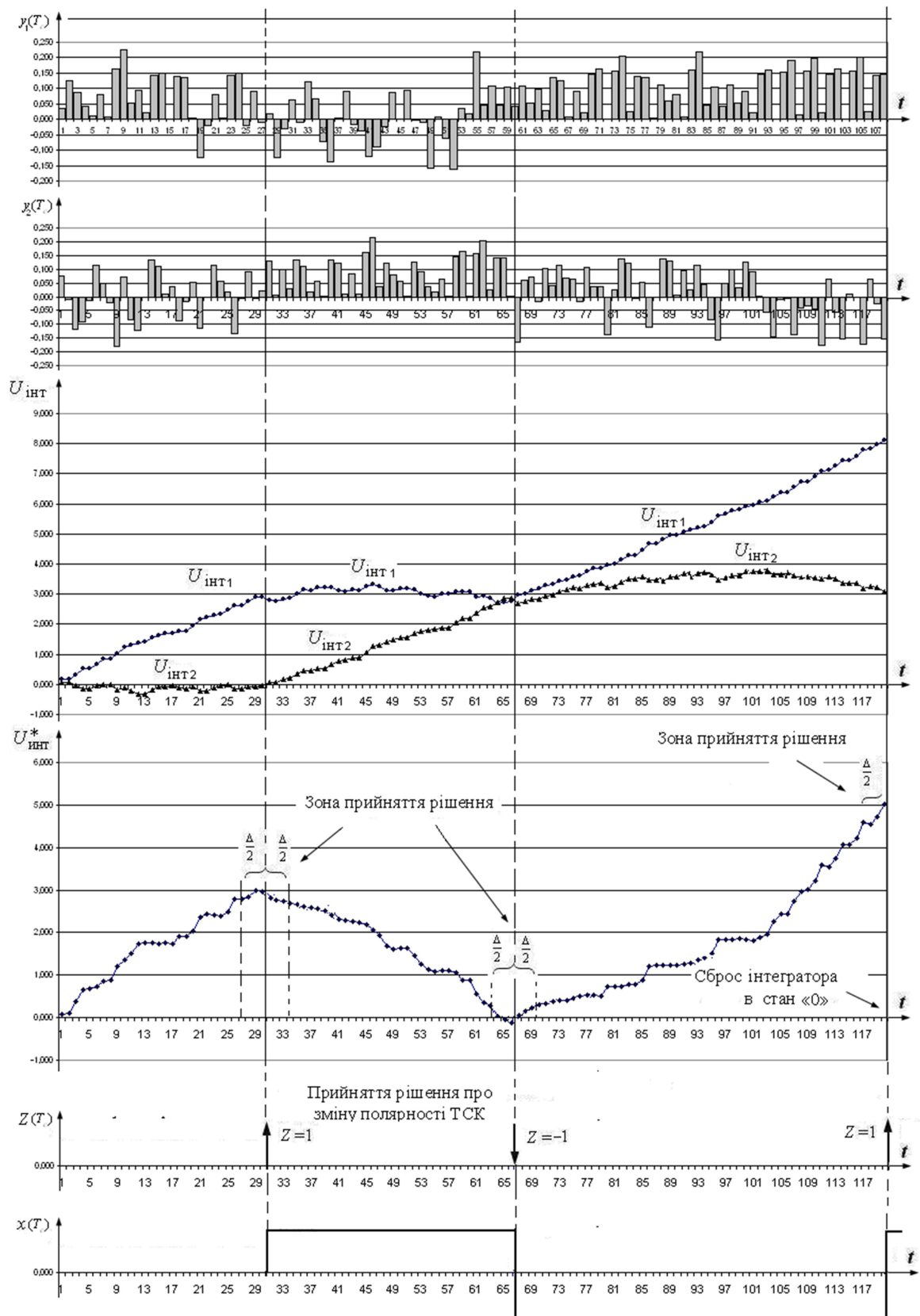


Рисунок 6.19 – Часові діаграми кореляційного приймання сигналу за допомогою двох розширювальних сигнатур $s_1(T_c)$ і $s_2(T_c)$

З одного боку, це ускладнює процес підбору відповідних хаотичних послідовностей, але з іншого – дозволяє істотно розширити ансамбль сигналів, які можуть застосовуватися для підвищення структурної та інформаційної прихованості при передаванні. Структурна прихованість синтезованої сигнальної конструкції з урахуванням кількості реалізацій N_p ТСК, а також показників прихованості $S_{\text{тск}}$ і $S_{\text{хск}}$, визначається за формулою:

$$S = N_p \times S_{\text{тск}} \times S_{\text{хск}}. \quad (6.59)$$

Отже, даний метод розширення спектра таймерних сигналів на основі хаотичних коливань забезпечує підвищення структурної СКК. Використання двох хаотичних послідовностей дозволяє точно фіксувати моменти зміни фронтів таймерного сигналу та підвищує завадостійкість системи. Збереження ортогональності хаотичних послідовностей є ключовою умовою ефективності методу. Запропонований підхід суттєво збільшує ансамбль можливих реалізацій сигналів і підсилює захист інформації в каналах зв'язку.

6.10. Дослідження енергетичної прихованості шумоподібних таймерних сигналів

Використання непозиційних таймерних сигналів [99, 154], а також систем модуляції з питомою швидкістю $\gamma_m > 1$, дає можливість значно підвищити не лише структурну, а й енергетичну прихованість сигнально-кодових конструкцій. У зв'язку з цим актуальним завданням є розробка методів формування широкосмугових шумоподібних сигналів на основі ТСК у поєднанні з ПВП, що використовують різні системи модуляції.

При побудові алгоритмів синтезу широкосмугових сигналів ключове значення має узгодження параметрів формування ТСК [153] з особливостями структури ортогональних ПВП та їх базою $B_{\text{пвп}}$. Ортогональні ПВП за своїми властивостями наближаються до шумоподібних сигналів, у яких мінімальна

тривалість елементарної послілки t_q значно менша за час передавання інформаційного елемента t_0 , тобто $V_{\text{інф}} \gg V_{\text{ПВП}}$, або $t_q \ll t_0$.

Для формування імпульсів таймерних сигналів використовується базовий елемент Δ , тривалість якого у s разів менша за тривалість елементарної послілки t_0 , але водночас перевищує мінімальну тривалість чіпа t_q .

Алгоритм прямого розширення спектра та вибір бази послідовності B ґрунтується на особливостях побудови таймерних сигналів. Як послідовності розширення пропонується застосовувати ортогональні послідовності Уолша. Відомо, що пряме розширення спектра інформаційного позиційного коду реалізується на кожному інтервалі t_0 за допомогою ПВП.

Однак застосування такого алгоритму до непозиційних кодів є неможливим, оскільки моменти модуляції таймерних сигналів, що формуються на інтервалі $T_c = nt_0$ (де n – кількість елементарних посилок), визначаються не кратністю t_0 , а базовим елементом Δ (де $\Delta = t_0/s$; $s = 1, 2, 3, \dots, l$ – цілі числа). Тому для непозиційних таймерних сигналів використовується псевдовипадкова послідовність розширення довжиною

$$B_{\text{ТСК}} = B_{t_0} \times n,$$

яка узгоджується з усім часовим інтервалом T_c при збереженні тактової частоти системи зв'язку. При цьому значення $B_{\text{ТСК}}$ повинно бути кратним числу:

$$N_{\Delta} = s \times n,$$

де N_{Δ} – кількість елементів Δ на інтервалі T_c .

Для прикладу розглянемо наступні варіанти побудови ТСК:

1) якщо $s = 4$, $n=4$, $N_{\Delta} = 16$, тоді для узгодження структури ТСК і ПВП потрібно, щоб $B = 32; 64; 128 \dots$;

2) якщо $s = 4$, $n=4$, $N_{\Delta} = 12$, тоді $B = 12; 24; 48 \dots$.

Зробимо аналіз процесу формування широкосмугового таймерного сигналу за наступними параметрами: $T = 4t_0$; $s = 2$.

Хай $x_k(t)$ інформаційний сигнал k -го користувача. Після завадостійкого кодування він перетворюється у кодовану послідовність $x_k^{\text{ПК}}(t)$, яка формувачем таймерних сигналів відображається у таймерний код $x_k^{\text{ТСК}}(t)$. Далі цей сигнал множиться на псевдовипадкову послідовність (ПВП) $s_k(t)$, що відповідає k -му користувачу. У результаті формується сигнал:

$$b_k(t) = x_k^{\text{ТСК}}(t) \cdot s_k(t), \quad (6,60)$$

який надходить на бінарний фазовий модулятор. На його виході кожен елемент ПВП перетворюється у фазоманіпульований сигнал:

$$s_k(t; b_k) = x_k^{\text{ТСК}}(t) \cdot s_k(t) \cdot \cos(2\pi f_0 t). \quad (6,61)$$

На рис. 6.20 представлено процес прямого розширення спектра сигнальної конструкції $x_k^{\text{ТСК}}(t)$ за допомогою сигнатури $s_k(t)$ для одного з індивідуальних каналів. У випадку фазової маніпуляції з двома станами (ФМ-2) одному символу відповідає один елемент ПВП, що визначає питому швидкість модуляції $\gamma_m = 1$.

Водночас можуть застосовуватися ансамблі двовимірних сигналів квадратурної амплітудної модуляції (QAM), які забезпечують щільнішу упаковку сигналів, при цьому $\gamma_m > 1$. Сигнальні конструкції вибираються з ансамблю, що містить $M_{\text{бл}}$ можливих варіантів.

Модуляція елементів тривалістю $t_{\text{ч}}$ розширеної таймерної сигнальної конструкції з полягає у наступному:

1) двійкова послідовність ТСК розбивається на блоки довжиною $n_{\text{бл}} = \log_2 M_{\text{бл}}$ символів $t_{\text{ч}}$.

2) загальна кількість можливих блоків довжини $n_{\text{бл}}$ дорівнює обсягу ансамблю $M_{\text{бл}} = 2^{n_{\text{бл}}}$;

3) кожному сигналу з ансамблю системи модуляції ставиться у відповідність конкретний блок двійкових елементів t_q .

Слід підкреслити, що вибір модуляційного коду визначається як конфігурацією ансамблю сигналів, так і характеристиками завад, які діють у каналі з багатопозиційною модуляцією. У випадку демодуляції багатопозиційних сигналів у каналі з гаусівським шумом найбільш імовірними є помилки типу «перехід», коли прийнятий сигнал сприймається як найближчий за мінімальною евклідовою відстанню.

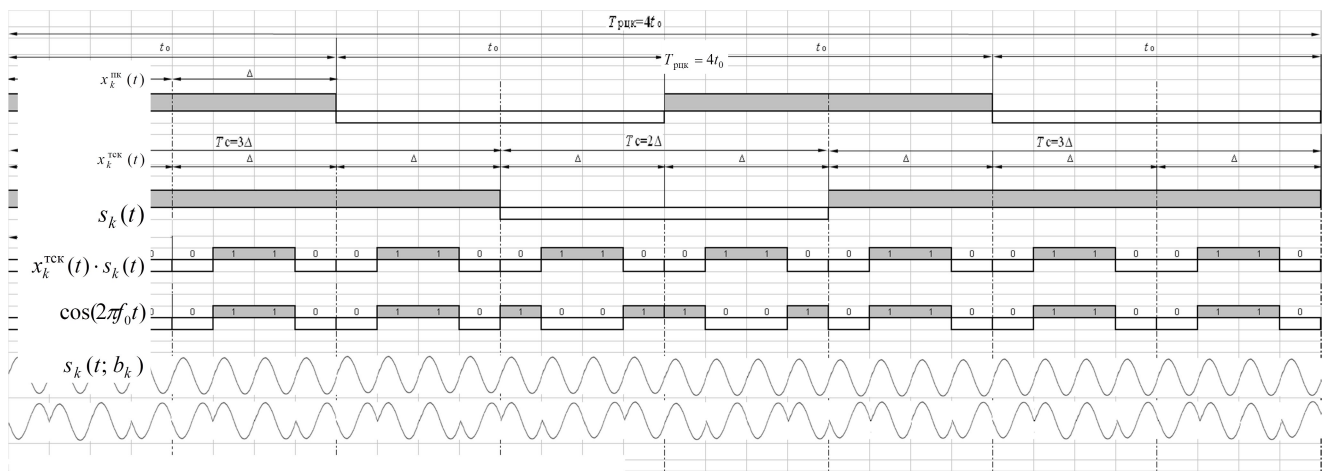


Рисунок 6.20 – Процес прямого розширення спектра сигнальної конструкції $x_k^{\text{тск}}(t)$ сигнатурою $s_k(t)$

Таймерні сигнали дозволяють виявляти та виправляти помилки за рахунок контролю зсуву фронтів у межах інтервалу $l_{\text{см}} = \pm(1 \dots 2)\Delta$, де часовий інтервал Δ у процесі розширення спектра вузькосмугового сигналу замінюється сегментами ПВП:

$$\Delta = l_{\Delta} t_q, \quad (6.62)$$

де l_{Δ} – кількість елементарних посилок тривалістю t_q , які формують інтервал часу Δ .

Отже, здатність ТСК до корекції помилок визначається щільністю заповнення інтервалу Δ елементами ПВП тривалості t_q .

Для прихованих методів передавання критерієм ефективності є максимізація апіорної невизначеності параметрів сигналів для засобів радіотехнічної розвідки. Енергетична прихованість оцінюється за критерієм досягнення у каналі максимального маскувального ефекту, коли енергія сигналу «розчиняється» на фоні шуму. Це можливо при мінімальному співвідношенні сигнал/шум $h^2 \leq 1$, за якого все ж забезпечується задана ймовірність приймання таймерного сигналу визначеної довжини.

Для шумоподібного таймерного сигналу $\vec{z}_n$ сформованого на основі прямого розширення спектра псевдовипадковими послідовностями Уолша з модуляцією ФМ-2, ФМ-4 та ФМ-8, проведено оцінку енергетичної прихованості у каналі з гаусівським шумом за умови кореляційного прийому.

Попередньо досліджувалася залежність ймовірності помилки на елемент ПВП від відношення сигнал/шум h^2 для різних значень бази сигналу B :

$$p_0 = 0,5 - \Phi_0(\sqrt{2} h), \quad (6.63)$$

де $\Phi_0(z)$ – інтеграл ймовірності.

Якщо на тривалості одного біта t_0 передається N_e елементів ПВП з тривалістю τ , то відношення сигнал/шум h^2 на біт на виході корелятора при прийомі повністю відомого сигналу зростає у $B = N$ разів.

На рис. 6.21 наведено графіки залежності ймовірності спотворення таймерного сигналу $P_{\text{П ТСК}}$ довжини $n = 7$ від відношення сигнал/шум за напругою $h^2 = \sqrt{E_0/N_0}$ та бази сигналу B .

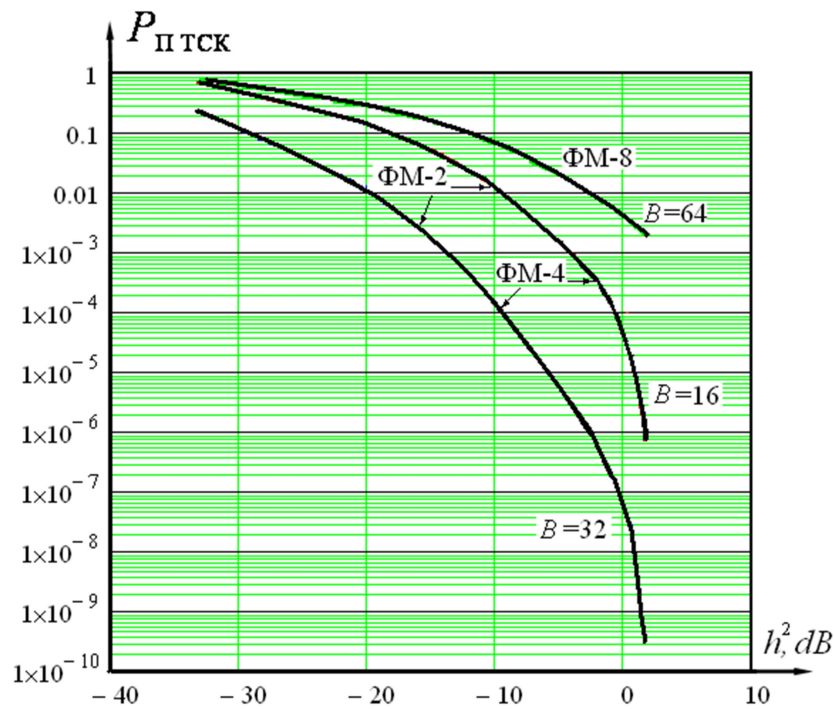


Рисунок 6.21 – Графіки залежності ймовірності спотвореної ТСК від B та h^2

Аналіз отриманих графіків показує, що на ймовірність спотворення таймерних сигналів $P_{\text{ПТСК}}$ впливають як тип модуляції, так і значення бази ВВВ. Результати для ФМ-2 та ФМ-4 практично збігаються, що пояснюється тим, що ФМ-4 є комбінацією двох систем ФМ-2 з несучими, зсунутими $\pi/2$. При цьому частотна ефективність каналу у ФМ-4 зростає вдвічі. Подальше підвищення позиційності модуляції (наприклад, ФМ-8) веде до істотного зростання ймовірності спотворень $P_{\text{ПТСК}}$ навіть при збільшенні бази до $B = 64$.

Експериментальні результати підтвердили, що у каналі з гаусівським шумом відновлення таймерного сигналу з $P_{\text{ПТСК}} = 10^{-4}$ для ФМ-2 при $B = 16$ можливе вже за відношення сигнал/шум 0 дБ. При 10 дБ і збільшенні бази до $B = 32$ ймовірність спотворень зменшується на три порядки, до $P_{\text{ПТСК}} = 10^{-7}$.

Отже, доведено, що використання шумоподібних ТСК забезпечує енергетичну прихованість, тобто передавання сигналів із рівнем напруги, співмірним або навіть нижчим за рівень шуму в каналі. Головною перевагою синтезованих шумоподібних таймерних сигналів є значне підвищення їх

структурної прихованості у порівнянні з позиційними шумоподібними сигналами. Проведені експерименти довели, що у каналі з гаусівським шумом відновлення таймерного сигналу з $P_{\text{ПТСК}} = 10^{-4}$ для ФМ-2 при $B = 16$ може здійснюватися при значенні відношення сигнал/шум 0 дБ, а при -10 дБ значення $P_{\text{ПТСК}} = 10^{-7}$ зменшується на три порядки при збільшенні бази до $B = 32$. Отже, доведено, що система з шумоподібними ТСК здатна забезпечити енергетичну прихованість, тобто здійснювати передавання з рівнем напруги сигналу в каналі співвимірних з рівнем шуму або меншим його. Перевага синтезованих шумоподібних таймерних сигналів полягає в значному підвищенні їх структурної прихованості в порівнянні з шумоподібними позиційними сигналами.

Висновки

У шостому розділі дисертації проведено дослідження та розроблено методи формування шумоподібних таймерних сигналів, спрямованих на забезпечення високого рівня енергетичної та структурної прихованості в умовах дії засобів радіоелектронної розвідки та активних завад.

1. Показано, що використання ТСК у поєднанні з методами прямого розширення спектра, ППРЧ, ЛЧМ, мультиплексування та хаотичних коливань дозволяє сформувати широкий клас сигналів з підвищеною завадостійкістю.

2. Встановлено, що вибір бази сигналу та алгоритму розширення спектра безпосередньо впливає на структурну прихованість та еквівалентну криптостійкість системи.

3. Розрахунки довели, що комбіновані методи (ПВП та ППРЧ, ТСК та ЛЧМ, ТСК та хаотичні послідовності) забезпечують зростання структурної прихованості у 1,5–2 рази порівняно з класичними підходами.

4. Імітаційне моделювання підтвердило можливість відновлення фронтів таймерних сигналів у каналах з низьким відношенням сигнал/шум, що забезпечує енергетичну прихованість навіть при $h^2 \leq 1$.

5. Запропонований метод мультиплексування ТСК дозволяє зменшити кількість піднесучих частот у порівнянні з OFDM, зберігши при цьому високу стійкість до завад і збільшивши прихованість передавання.

6. Використання хаотичних сигналів для формування сигнальних конструкцій дозволяє значно розширити ансамбль можливих реалізацій, що ускладнює несанкціонований доступ і забезпечує підвищення рівня інформаційної безпеки.

Таким чином, у розділі обґрунтовано, що синтез шумоподібних таймерних сигналів на основі інтегрованих методів модуляції та розширення спектра є ефективним підходом для побудови захищених каналів зв'язку, які одночасно відповідають вимогам енергетичної та структурної прихованості.

ВИСНОВКИ

У дисертаційній роботі наведено нове вирішення науково-технічної проблеми підвищення захищеності ІКС. Обґрунтовано доцільність комплексного підходу до захисту інформації від НСД. Надано оцінку комбінованим методам захисту інформації в умовах радіоелектронного конфлікту. Запропоновано відповідні критерії й показники ефективності методів передавання даних на основі розроблених алгоритмів розширення спектра таймерних сигналів.

Отримано нові наукові й практичні результати, що полягають в такому:

1. Уперше запропоновано модель оцінювання захищеності передачі інформації на основі обсягу сигналу, яка дозволяє наочно оцінювати відповідність характеристик сигналу можливостям каналу та приймати рішення щодо методів узгодження або параметричного перетворення сигналу. Це дозволяє здійснювати оцінку рівня захищеності з урахуванням ресурсів каналу, що полягає в такому: найбільша енергетична прихованість у того метода передавання, який при заданій смузі широкосмугового сигналу ΔF і заданій достовірності передавання інформації забезпечує найменше співвідношення сигнал/шум h_0^2 , тобто $\min h_0^2 = E\{\Delta F; P_{\text{НП}}(n)\}$; найбільша потенційна структурна прихованість у того метода формування сигнальних конструкцій, який на заданому інтервалі часу побудови сигнальних конструкцій $T_{\text{СК}}$ і необхідної достовірності передавання забезпечує можливість синтезу більшого числа комбінацій A , тобто $\max A = S\{T_{\text{СК}}; P_{\text{НП}}(n)\}$.

Уперше запропоновано узагальнену модель вдосконалення методів прихованого передавання інформації, яка дозволяє здійснювати порівняльний аналіз методів захисту за критеріями прихованості та завадостійкості.

2. Уперше запропоновано метод взаємного обміну якості та швидкості передавання інформації шляхом комбінованого застосування таймерних і позиційних кодів у нестаціонарних каналах зв'язку, що дозволяє підвищити

захищеність та ефективність систем зв'язку в умовах радіоелектронного конфлікту. Дослідження показали, що використання таймерних сигналів з параметрами $m = 5$, $s = 7$, $N_{\text{ТСК}}=680$ забезпечує збільшення відносної швидкості передавання інформації на інтервалах «хорошого» стану каналу (відношення сигнал/шум $h = 12$, $P_{\text{ТСК}} = 1,79 \times 10^{-4}$) з $R_{\text{РЦК}}=0,55$ для РЦК з параметрами $n = 9$, $m = 5$, $t_{\text{в}} = 1$, $N_{\text{РЦК}}=512$, $P_{\text{РЦК}} = 1,4 \times 10^{-2}$ до $R_{\text{ТСК}}=1,88$. Це свідчить про те, що використання таймерних сигналів на інтервалі «хорошого» стану каналу дозволяє зменшити час передавання інформації в три рази і більше. Сумісне використання ТСК і РЦК дозволяє підвищити завадостійкість в 1,59 рази при збільшенні $R_{\text{РЦК}} = 0,55$ до $R_{\text{РЦК-ТСК}} = 1,05$, що свідчить про зменшення часу передавання заданого обсягу інформації в два рази.

3. Уперше запропоновано метод одночасного захисту інформації від НСД та випадкових завад у каналі зв'язку, що дозволило встановити залежність рівня структурної прихованості ТСК та завадостійкості від мінімальної кодової відстані дозволених комбінацій, які визначаються як за рівнянням якості, так і шляхом повного перебору всіх можливих сигнальних конструкцій. Доведено, що збільшення структурної прихованості можливо на обмеженому інтервалі часу передавання інформації за допомогою таймерних сигналів у порівнянні з позиційними кодами. Так, для $n = 7$, $i = 3$ і $s = 5$ число реалізацій $N_{\text{р}}=1771$ та структурної прихованості $S_{\text{ТСК}} = 11$, тоді як для РЦК всього $N_{\text{РЦК}}=2^7=128$ та $S_{\text{РЦК}} = 7$. Визначено, що використання ТСК в якості завадостійкого коду з мінімальною кодовою відстанню $d_0 = 2, 3, 4, 5$ зменшує кількість дозволених комбінацій у порівнянні з $N_{\text{р}}=1771$ в 2, 7, 12, 22 рази відповідно. Така закономірність характерна для множин ТСК з іншими параметрами n , i та s . Результати дослідження дали змогу виявити зворотну закономірність між показниками структурної прихованості і завадостійкості, що пов'язана із зменшенням базового елементу побудови таймерних сигналів Δ або/та збільшення кодової відстані. Для вирішення цієї проблеми запропоновано використання більшої кількості різних множин ТСК у процесі передавання інформації. Такий підхід дозволяє компенсувати зменшення показника

структурної прихованості при обмеженому значенні Δ та кодової відстані, які потрібні для забезпечення заданої достовірності.

4. Уперше розроблено багаторівневу модель захисту інформації, яка забезпечує синергетичне поєднання статистичного шифрування, завадостійкого та таймерного кодування, а також процедури декореляції помилок. Такий підхід дозволяє одночасно на кожному рівні моделі підвищити криптостійкість, завадостійкість та захист від НСД. Запропоновано враховувати ентропію дискретного джерела інформації для визначення кількості випадкових комбінацій для кожного символу b_j алфавіту залежно від ймовірності його появи. Такий підхід штучно змінює ентропію джерела видачі інформації з нерівномірним законом появи символів у повідомленні з $H_{\text{HP}}(U) = 4,42$ до $H_{\text{P}}(U) = 5$ (для алфавіту з 32 символів) та забезпечує рівноймовірний закон появи кодових комбінацій у шифрограмі. Оцінку ефективності стохастичного шифрування зроблено на основі імітаційного моделювання для порівняльного аналізу варіантів залежно від загальної кількості використовуваних випадкових комбінацій N_1 та довжини випадкової комбінації n . Визначено, що варіант реалізації системи стохастичного шифрування, у якому використовується підбір випадкових кодових комбінацій шифрограми з урахуванням ймовірності появи символу в тексті дозволяє зменшити дисперсію залежно від довжини кодової комбінації $n=9, 10, \dots, 17$ у межах від 28, 47, $\dots$, 57269 рази відповідно, що забезпечує зменшення дисперсії $D_{xy} \rightarrow 0$. Це дозволяє формувати потік випадкових комбінацій шифрограми з приблизно рівними ймовірностями появи та ускладнити використання частотного тесту при дешифруванні перехопленого повідомлення. Для компенсації надлишковості випадкових комбінацій стохастичного шифрування і блокового кодування запропоновано використання ТСК.

5. Уперше встановлено закономірності впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Визначено, що з погляду зменшення складності прийому шумоподібних таймерних сигналів доцільно використовувати фіксоване значення ЗММ i ,

кількість реалізацій яких при цьому залежить від інтервалів Найквіста m та елементів s . Аналіз впливу фіксованої кількості ЗММ в ТСК дозволяє зробити висновок, що максимальна кількість реалізацій може бути досягнута при певному значенні i , яке, як правило, менше m на 2-4 позиції. Визначено вплив зростання числа реалізацій ТСК при збільшенні інтервалів побудови $m = 6, 7, \dots, 19$, що дозволяє підвищити структурну прихованість $S(s=7, i=4)$ в межах від 12 до 22 дв. вим. Збільшення кількості реалізацій можливо шляхом використання ТСК з різним ЗММ, що дозволяє підвищити структурну прихованість. Так при $S(m=19, s=6, i=1, 2, \dots, 19) = 40$ дв. вим., що у порівнянні з $S(m=19, s=6, i=4) = 21$ дв. вим. більше майже у 2 рази. Обґрунтовано вибір оптимального значення параметра $s_{\text{опт}}$ залежно від h^2 в каналі, при якому забезпечується максимальна пропускна здатність $C_{\text{тск}}$. Визначено, що зменшення часового інтервалу Δ при $s > s_{\text{опт}}$ для числа реалізацій ТСК та підвищення прихованості призводить до збільшення показника втрат H_3 , який характеризує збільшення спотворених сигнальних конструкцій. Отже, виявлено протиріччя між умовою підвищення структурної прихованості шляхом збільшення s та необхідністю обмеження цього показника значенням $s \leq s_{\text{опт}}$ при заданому m та відношенням сигнал/шум h .

6. Розвинуто теорію систем зв'язку з шумоподібними сигналами на основі ТСК, що пов'язано з розробкою нових алгоритмів розширення спектра для непозиційних сигналів та визначенням оптимальних параметрів таймерних сигналів. Запропоновано три умови забезпечення енергетичної прихованості для методів розширення спектра (ППРЧ, ПРС-ПВП та ЛЧМ) за критеріями частотної та енергетичної ефективності використання каналу: база сигналу $B = \Delta f T \gg 1$ – перша умова; частотна ефективність $\gamma = R / \Delta f_{\text{эф}}$ – друга умова; ефективність використання каналу відповідно до потужності $\beta = R / h_0^2$ – третя умова. Аналіз показав, що методи ППРЧ та ЛЧМ задовольняють тільки двом умовам, а метод ПРС-ПВП задовольняє всі умови. З урахуванням особливостей побудови ТСК запропоновано загальний принцип розширення спектра на інтервалі часу побудови сигнальної конструкції T_c , що пояснюється

непозиційністю імпульсів у порівнянні з позиційними РЦК. На загальне значення структурної прихованості ПРС-ПВП впливає структурні прихованості ТСК, ПВП та системи модуляції. При параметрах ТСК $m = 8$, $s = 5$, $i = 3$ структурна прихованість $S_{\text{ТСК}} = 12$ дв. вим. Розширення спектра ТСК методом ПРС-ПВП ($B_{t_0} = 8$, $N_{\text{ПВП}} = 64$) та використання ФМ-2 дозволяє досягти значення структурної прихованості $S_{\text{ТСК ПВП}} = 77$ дв. вим. При базі ПВП $B_{t_0} = 16$ та $N_{\text{ПВП}} = 128$ структурна прихованість шумоподібного таймерного сигналу збільшується практично в 2 рази $S_{\text{ТСК ПВП}} = 141$ дв. вим. При формуванні ШПС структура ПВП змінюється і становиться унікальною після розширення спектра кожної ТСК.

Надано аналіз структурної прихованості шумоподібного ТСК при розширенні спектра методом ППРЧ. Використання швидкої ППРЧ дозволяє при параметрах ТСК $m = 4$, $s = 4$ та незначної кількості частот $N_f = 32$ забезпечити наступну структурну прихованість $S_{\text{ТСК ППРЧ бп}} = 73,4$ і $S_{\text{ТСК ППРЧ п}} = 80$ для системи зв'язку з повторення та без повторенням несущих частот відповідно.

При комбінованому розширенні спектра на основі ПРС-ПВП і ППРЧ структурна прихованість шумоподібного таймерного сигналу збільшується в 2 рази і більше. Розширення спектра ТСК з параметрами $m = 8$, $s = 5$, $N_{\text{ПВП}} = 32$; $i = 3$, $N_{\text{ПВП}} = 64$, $N_f = 32$ забезпечує структурну прихованість $S_{\text{ТСК ПВП-ППРЧ}} = 157$ дв.вим. При інтерпретації структурної прихованості з криптостійкістю можна зробити висновок, що значення $S_{\text{ТСК ПВП-ППРЧ}} = 157$ дв. вим. перевищує криптостійкість системи шифрування DES з довжиною ключа $k_{\text{DES}} = 56$ та AES з $k_{\text{AES}} = 128$. Надано імітаційне моделювання розширення ТСК за допомогою ЛЧМ, що дало змогу з'ясувати, що відновлення фронтів сигнальної конструкції можливо при значенні $h = 0,25$ на вході приймача, тобто коли шум перевищує корисний сигнал у 4 рази.

Розроблено нові алгоритми кореляційного прийому широкосмугових таймерних сигналів (для ПРС-ПВП та ЛЧМ), які враховують структуру побудови непозиційних сигналів.

Висока ефективність розроблених теоретичних положень, запропонованих методів захисту інформації на основі стохастичного шифрування і способів розширення спектра ТСК підтверджені результатами експериментальних досліджень, які одержано методами аналітичного та імітаційного моделювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кільдішев В.Й. Система оцінок захищеності методів захисту інформації в умовах РЕБ. *Забезпечення кібероборони держави*: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року. м. Київ. К.: НУОУ, 2023. С 65-68.
2. Горохов С. М., Захарченко М. В., Корчинський В. В. Критерії ефективності прихованих методів передачі. *Цифрові технології*: зб. наук. пр. Одес. нац. акад. зв'язку ім. О. С. Попова. Одеса, 2012. Вип. 12. С. 147–150.
3. Андрущенко О. Ю. Використання адаптивних алгоритмів для підвищення стійкості систем зв'язку. *Військово-технічний збірник*. 2021. №8. С. 22–29.
4. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення – 02.11.2023).
5. Боднар І. Р. "Інформаційна безпека як основа національної безпеки." *Mechanism of Economic Regulation*. №1. 2014. с. 68-75.
6. Гнатюк С. О., Рябий М. О., & Лядовська В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту : аналіз підходів. *Зв'язок*. №4, с. 3-7.
7. Григоренко, П. О., Соловей, Т. І. Сучасні технології передачі інформації в умовах радіоелектронних загроз. *Інформаційні системи в умовах загроз* : Матеріали міжнародної науково-практичної конференції. КПІ ім. І. Сікорського. (м. Київ, 25–27 березня 2023 р.). Київ. 2023, с. 89–92.
8. Мельник, А. Ю., Шевченко, В. І. Аналіз технологій глушіння сигналів в умовах РЕБ. *Інформаційна безпека та кіберзахист* : Всеукраїнська наукова конференція. ОНУ ім. І. І. Мечникова. (м. Одеса, 14–16 червня 2022 р.) Одеса. 2022, с. 57–60.

9. Особливості застосування технологій РЕБ у військових конфліктах. *Науковий портал України*. URL: <https://www.science-ukraine.com/rew-2024> (дата звернення: 01.12.2024).
10. Лісовський П. М., Лісовська Ю. П. Криптосистема військ радіоелектронної боротьби України. Військове право : навч. посіб. Київ : Ліра-К, 2024. 130 с.
11. Shamanov D., Sorokin A. Аналіз сучасних методів радіоелектронної боротьби. Збірник наукових праць «Системи управління, навігації та зв'язку». Полтава : ПНТУ, 2024. Т. 1 (75). С. 211–214.
12. Пічугін М. Ф., Носова Г. Д. Аналіз тактики застосування підрозділів РЕБ у сучасних війнах та локальних збройних конфліктах. *Збірник наукових праць ЖВІ НАУ*. Київ, 2010. Вип. 3.
13. Семененко О. М., Бойко Р. В., Добровольський Ю. Б., Іванов В. Л., Кремешний О. І. Контррадіоелектронна боротьба як складова частина радіоелектронної боротьби в Збройних Силах України. *Системи озброєння і військова техніка*. 2016. Вип. 46. С. 141–145.
14. Камінський А. А. Теорія і практика радіоелектронної боротьби : навч. посіб. Київ : НАУ, 2016. 240 с.
15. Тимошенко В. І. Радіоелектронна боротьба: навч.-метод. посіб. Харків : ХНУПС, 2017. 176 с.
16. Сидоренко О. В. Сучасні аспекти радіоелектронної боротьби. *Досвід і перспективи*. Київ : ВПЦ «Київський університет», 2020. 220 с.
17. Гурський Т. Г., Жук О. Г., Клімович С. О. Напрямки застосування псевдовипадкових послідовностей в радіомережах спеціального призначення. *Вісник Хмельницького національного університету*. 2012. № 6. С. 160–167.
18. Крижний А. В., Гурський Т. Г., Климович С. О. Аналіз характеристик систем радіозв'язку з використанням кодового розділення каналів. *Збірник наукових праць Національної академії державної прикордонної служби України. Серія : військові та технічні науки*. 2014. № 1(61). С. 342–356.

19. Poisel R. A. Modern Communications Jamming: Principles and Techniques. *Boston : Artech House*. 2011. 450 p.
20. Наконечний Т. А., Євграфов Д. В. Перехоплення сигналу витoku інформації з екрану монітора. *Захист інформації*. 2021. Т. 23, № 3. С. 160–167.
21. Дюжев, В. Г. Методи розширення спектра сигналів: теорія та застосування. *Наукова думка*. Київ. 2018. 356 с.
22. Гуржій, А. М., Колесников В. В. Проблеми та рішення підвищення завадостійкості систем зв'язку. *Вісник НТУУ «КПІ». Серія: Радіотехніка*. 2021. №2. С. 15–22.
23. Сталій розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б.В. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. Одеса : ДУ «ІРЕЕД НАНУ», 2024. 543 с.
24. Adamy, D. L. EW 101: A First Course in Electronic Warfare. *Boston: Artech House*. 2001. 320 p.
25. Poisel, R. A. Modern Communications Jamming: Principles and Techniques. *Boston: Artech House*. 2011. 450 p.
26. Schleher, D. C. Electronic Warfare in the Information Age. *Boston: Artech House*. 1999. 550 p.
27. Knott, E. F., Shaeffer, J. F., Tuley, M. T. Radar Cross Section. *2nd ed. Boston: Artech House*. 2004. 590 p.
28. Лисенко О. П., Бондар А. І. Моделювання завадостійких методів передачі сигналів у умовах РЕБ. *Збірник наукових праць НТУ «ХПІ»*. 2022. №1. С. 33–40.
29. Бобровський А. П. Основи радіоелектронних систем. *Техніка*. Київ. 2019. 312 с.
30. Коваленко І. М. Особливості застосування методів радіоелектронної боротьби в сучасних конфліктах. *Вісник Харківського університету повітряних сил ім. І. Кожедуба*. 2022, № 2(64), с. 45–50.

31. Hordiichuk V., Korchynskyi V., Kildishev V., Zakharchenko M. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods. 2022 *IEEE 2nd Ukrainian Microwave Week (UkrMW)*. Kyiv, 14-18 Nov. 2022. P. 331–334.

32. Захарченко М.В., Корчинський В.В., Радзімовський Б.К., Горохов Ю.С. Ефективність прямого розширення спектра в системах зв'язку з таймерними сигналами. *Вісник НУ «Львівська політехніка»*. 2015. № 818. С.76–79.

33. Лізунов С. І., Кадулін М. О. Використання аналізаторів спектра для захисту інформації. *Запорізький національний технічний університет. Тиждень науки-2019*. Факультет радіоелектроніки та телекомунікацій. Збірник тез доповідей щорічної науково-практичної конференції. 15-19 квітня 2019 року. С. 110–112.

34. Наконечний Т. А., & Євграфов Д. В. Перехоплення сигналу витoku інформації з екрану монітора. *Захист інформації*. Том 23, №3, липень-вересень 2021. С. 160-167.

35. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах. *Математичне та комп'ютерне моделювання*. Серія: Технічні науки : зб. наук. Праць. Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

36. Мандзій Б. А., Желяк Р. І. Основи теорії сигналів : підручник / за ред. Б. А. Мандзія. Львів : Видавничий дім «Ініціатива», 2008. 240 с.

37. Політанський Л. Ф., Політанський Р. Л., Рождественська М. Г., Гресь О. В. Система передавання даних з використанням псевдовипадкових послідовностей у кодах Хемінга. *Сучасні інформаційні та електронні технології* : тр. XII міжнар. наук.-практ. конф. Одеса, трав. 2011. С. 156.

38. Корчинський В.В, Рябуха О.М, Аль-Файюмі ХАЛЕД, Гавель С.М Дослідження варіаційних можливостей генераторів хаосу по формуванню

псевдовипадкових послідовностей. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. 2023. № 1 С. 180–186.

39. Алімов О. І. Радіoeлектронна боротьба: основи теорії та практики. *НВП «Наука і техніка»*. Київ. 2020. 368 с.

40. Ключко, А. В., Іванов, С. В. Радіoeлектронна розвідка та боротьба : сучасні підходи. *Харківський університет повітряних сил*. Харків. 2021. 290 с.

41. Захарченко М.В., Горохов С.М., Балан М.М., Гаджієв М.М., Корчинський В.В., Ложковський А.Г. Математичні основи оптимізації телекомунікаційних систем : підручник / ред. М.В. Захарченко. Одеса : ОНАЗ ім. О.С. Попова. 2010. 240 с.

42. Proakis, J. G., & Manolakis, D. K. *Digital Signal Processing: Principles, Algorithms, and Applications* : 4th ed. – Upper Saddle River, NJ: Prentice Hall, 2007. 1002 p.

43. Sklar, B. *Digital Communications: Fundamentals and Applications*. Upper Saddle River. NJ: Prentice Hall, 2001. 1100 p.

44. Zakharchenko N., Korchinsky V., Radzimovsky B. Information security of Time-Controlled Signals in Confidential Communication Systems. *Modern problems of radio engineering, telecommunications and computer science* : XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012) Lviv. Publishing House of Lviv Polytechnic. 2012. P. 317.

45. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaioni Kh. Method of information protection based on the integration of probabilistic encryption and noise immune coding. *Radioelectronic and Computer Systems*. 2023. Vol. 4, No. 13. P. 184–196.

46. Serkov, A., Kasilov, O., Lazurenko, B., Pevnev, V., Trubchaninova K. Strategy of building a wireless mobile communication system in the conditions of electronic counteraction. *Radioelectronic and computer systems*. 2023. No 2 (106). P. 160–170. DOI: 10.32620/reks.2023.2.13.

47. Avramenko, V., Demianenko, V. Serial encryption using the functions of real variable. *Radioelectronic and computer systems*. 2021. No 2(98). P. 39–50. DOI: 10.32620/reks.2021.2.04.

48. Захарченко М. В., Гаджієв М.М., Б. К. Радзімовський, Горохов Ю. С., Шпак Д. О. Порівняння синдромних методів для коригуючих блокових позиційних і таймерних кодів. *Восточно-Европейский журнал передовых технологий*. 2014. № 2/9(68). С. 4–8.

49. Hordiichuk V., Shyshatskyi A., Korchynskyi V., Kildishev V. Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems. *Journal of Physics: Conference Series*. 2021. Vol. 1839. P. 1–10.

50. Korchynskyi V. V., Kildishev V. I., Holey D. V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding. *Radio Electronics, Computer Science, Control*. 2019. No. 3 (50). P. 108-116.

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

52. 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.

53. Кононович В.Г., Тардаскін М.Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування. *Захист інформації*. № 1. 2006. 18–30 с.

54. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах НД від несанкціонованого доступу : Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. 57 с.

55. Богуш В.М., Юдін О.К. Інформаційна безпека держави : навч. посіб. Київ : «МК-Прес», 2005. 432 с.

56. Захарченко М. В., Кільдішев В. Й., Белова Ю. В., Хомич С. В. Вплив корельованих завад на пропускну здатність безперервного каналу зв'язку.

Вісник НТУ «ХПІ». Серія : Нові рішення у сучасних технологіях. 2012. Вип. 33. С. 62–68.

57. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Осадчук К. О. Інформаційні параметри кодів Сліп'яна з компенсацією надмірності таймерними сигналами. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 1. С. 14-20.

58. Zakharchenko N. V., Korchinskiy V. V., Radzimovskiy B. K., Bektursunov D. N., Gorokhov Y. S. Assessing the impact of the noise on the throughput communication channel with timing signals. *Eastern European Scientific Journal*. Düsseldorf : AURIS Kommunikations- und Verlagsgesellschaft mbH, 2015. № 4. С. 209–214.

59. Корчинський В. В., Назаренко О. А., Степанов В. О., Аль-Файюмі Халед. Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів. *Інфокомунікаційні та комп'ютерні технології*. Київ : Відкритий міжнар. ун-т розвитку людини «Україна», 2022. № 2 (02). С. 25–31.

60. Корчинський В. В., Кільдішев В. Й., Аль-Файюмі Халед, Валігурський Ю. П. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції. *Перспективні напрямки захисту інформації* : матеріали сьомої міжнар. наук.-практ. конф., м. Одеса, 30 серп. – 3 верес. 2021 р. Одеса–Тернопіль : Вид-во «Крок», 2021. С. 31–33.

61. Корчинський В. В., Кільдішев В. Й., Хомич С. В., Белова Ю. В. Ефективність j -кратного повторення надлишкових таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ»*. 2012. Вип. 26. С. 88–95.

62. Kempf M., Gauder N., Jaeger B., Zirngibl J., Carle G. A quantum of QUIC: Dissecting cryptography with post-quantum insights [Електронний ресурс]. *arXiv preprint*, 2024. – Режим доступу : <https://arxiv.org/abs/2405.09264>

63. Song K., Imran N., Chen J. Y., Dobbins A. C. A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications. *arXiv preprint*. 2025. Режим доступу: <https://arxiv.org/abs/2504.08618>.

64. Perugini L., Vesco A. An Efficient TLS 1.3 Handshake Protocol with VC Certificate Type. arXiv preprint. 2024. Режим доступу: <https://arxiv.org/abs/2407.12536>.
65. Battarbee C., Striecks C., Perret L., Ramacher S., Verhaeghe K. Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication. arXiv preprint. 2024. Режим доступу: <https://arxiv.org/abs/2411.04030>.
66. Shannon C. E. A Mathematical Theory of Communication. University of Illinois Press, 1948. 144 p.
67. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaioni Kh. Method of information protection based on the integration of probabilistic encryption and noise immune coding. *Radioelectronic and Computer Systems*. 2023. Vol. 4, No. 13. P. 184–196.
68. Корчинський В. В., Рябуха О. М., Аль-Файюмі Х. О., Василенко А. Ю. Метод захисту інформації на основі ймовірнісного шифрування. *78-а науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів*. Одеса : ДУІЗ, 21–22 листопада 2023.
69. Корчинський В. В., Рябуха О. М., Бердніков О. М., Аль-Файюмі Х., Поліщук К. В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції. *Перспективні напрямки захисту інформації* : матеріали сьомої міжнародної науково-практичної конференції, м. Одеса. 30 серпня – 3 вересня 2021 р. Одеса–Тернопіль : Видавництво «Крок», 2021. С. 27–30.
70. Горохов Ю. С., Корчинський В. В., Рудий Е. М. Метод кодового розділення каналів на основі таймерних сигнальних конструкцій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2016. № 1. С. 208–211.
71. Корчинський В. В., Аль-Файюмі Х., Копитін Ю. В., Копитіна М. В., Валигурський Ю. П. Прогнозування та оцінки ризиків інсайдерських загроз. *Перспективні напрямки захисту інформації* : матеріали шостої міжнародної всеукраїнської науково-практичної конференції, 2–6 вересня 2020 р., Одеса. Одеса : Бондаренко М. О. ОНАЗ, 2020. С. 64–65.

72. Корчинський В. В., Аль-Файюмі Х. Мінімізація ризиків інсайдерських загроз в системах захисту. *Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів*, 12–14 грудня 2019 р., Одеса. Одеса : ОНАЗ ім. О. С. Попова, 2019. Ч. I. С. 139.

73. Корчинський В. В., Аль-Файюмі Х., Копитін Ю. В., Копитіна М. В. Ризики інсайдерських загроз у системах захисту інформації підприємств. *Наукові праці ОНАЗ ім. О. С. Попова*. 2019. № 2. С. 112–116.

74. Корчинський В. В., Кільдішев В. Й. Захищеність систем зв'язку спеціального призначення. *Проблеми інформатизації: матеріали п'ятої міжнародної науково-технічної конференції*, 13–15 листопада 2017 р., Черкаси. Черкаси : ЧДТУ, 2017. С. 18–19.

75. Корчинський В. В., Кільдішев В. Й. Підвищення прихованості передачі в системі зв'язку з кодовим розділенням каналів на основі динамічного хаосу. *Безпека інформації у інформаційно-телекомунікаційних системах* : матеріали XIX міжнародної науково-практичної конференції, 25–26 травня 2017 р., Буча. Буча : Держспецзв'язок, 2017. С. 48.

76. Корчинський В. В., Кільдішев В. Й., Бердніков О. М., Осадчук К. О. Підвищення захищеності системи зв'язку з таймерними сигнальними конструкціями та псевдовипадковою перебудовою робочої частоти. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 2. С. 179-182.

77. Корчинський В.В., Кільдішев В.Й., Бердніков О.М. Методи розширення спектру таймерних сигналів на основі псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації* : матеріали IV Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса : ОНАЗ. 2017. С. 57-59.

78. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Валігурський Ю.П. Метод порівняльного аналізу генераторів псевдовипадкових чисел.

Перспективні напрями захисту інформації : матеріали IV Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса : ОНАЗ. 2017. С. 46–48.

79. Korchynskii V. V., Osadchuk E. A., Kildishev V. I. Method of multiplexing of timer signal structures based on OFDM technology. *Вісник Національного університету «Львівська політехніка»*. 2017. № 2. Р. 41–44.

80. Корчинський В.В., Кільдішев В.Й., Осадчук К.О., Русаловська О.А. Підвищення захищеності передачі інформації на основі таймерних сигнальних конструкцій та технології OFDM. *Перспективні напрями захисту інформації* : матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса : ОНАЗ. 2017. С. 39–42.

81. Кільдішев В.Й., Бердніков О.М., Степанов В.О. Підвищення захищеності системи зв'язку з ППРЧ на основі таймерних сигнальних конструкцій. *Проблеми інформатизації* : п'ята міжнар. наук.-техн. конф. (м. Черкаси, 13–15 листопада 2017 р.). Черкаси : ЧДТУ. 2017. С. 17–18.

82. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Русаловська О.А. Спектральні методи захисту інформації на основі таймерних сигналів та псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації* : матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса : ОНАЗ, 2017. С. 36–39.

83. Корчинський В.В., Кільдішев В.Й., Бердніков О.М. Методи підвищення захищеності систем зв'язку на основі таймерних сигналів. Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів, тези доповідей. Одеса: ОНАЗ. 2017. С. 114–117.

84. Корчинський В.В., Кільдішев В.Й., Валігурський Ю.П., Поліщук К.В. Підвищення ефективності потокового шифрування в радіомережах на основі динамічного хаосу. Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів, тези доповідей. Одеса: ОНАЗ. 2017. С. 117–118.

85. Захарченко М.В., Корчинський В.В., Кільдішев В.Й. Про доцільність застосування зворотного зв'язку в системах передачі даних. Матеріали 64-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів (м. Одеса, 1–4 грудня 2009 р.). Одеса : ОНАЗ. 2009. С. 78–80.

86. Лунтовський А.О., Захарченко М.В., Семенко А.І. Мультисервісні мобільні платформи. Київ : ПБП «Задруга». 2014. 214 с.

87. Onyshchuk V., Kildishev V., Korchynskyi V. and Khaled Alfaiomi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services. *Telecommunications and Computer Engineering (TCSET) : Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics. (Ukraine February 22-26, 2022). Lviv-Slavske. 2022. P. 331-334.*

88. Гольдвассер Ш., Мікалі С. Ймовірнісне шифрування та семантична стійкість. *Журнал криптографічних досліджень*. 1982. №3. С. 45–65.

89. Гольдвассер Ш., Мікалі С. Криптографія: теоретичні основи та ймовірнісне шифрування. Київ : Вид-во технічної літератури. 2010. 280 с.

90. Савчук М. М. Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень : звіт про НДР. Київ : Фізико-технічний інститут, 2016. 120 с.

91. Голдвассер С., Мікалі С. Криптографія та теорія обчислень. Київ : Наукова думка, 2016. 320 с.

92. Молдован А. Гомофонний шифр: принципи побудови та застосування. *Журнал криптографічних досліджень*. 2002. № 4. С. 56–72.

93. Захарченко М. В., Кільдішев В. Й., Хомич С. В., Пришляк О. Г. Компенсація надлишковості в блокових коректуючих кодах за рахунок таймерних сигналів. *Вісник Хмельницького національного університету*. 2011. Вип. 2. С. 178–185.

94. Горохов Ю. С., Бектурсунов Д. Н., Захарченко М. В., Корчинський В. В., Радзімовський Б. К. Оцінка потужності таймерних кодів з урахуванням кількості інформаційних відрізків і значення твірного елемента Δ .

Вимірювальна та обчислювальна техніка в технологічних процесах. 2015. № 2. С. 198–201.

95. Захарченко М. В., Горохов Ю. С., Кріль А. С., Ковальчук С. В. Кодове ущільнення при таймерних сигналах. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2015. № 3 (24). С. 38–42.

96. Корчинський В. В. Оцінка структурної скритності сигнальних конструкцій на основі хаотичних сигналів у системах передачі конфіденційної інформації. Одеса : Наукові праці ОНАЗ ім. О. С. Попова. 2012. № 1. С. 77–81.

97. Корчинський В., Мар'ян М., Богданюк І., Аль-Файюмі Х. Метод захисту інформації від несанкціонованого доступу на основі динамічного хаосу. *Scientific Collection «InterConf»*. 2024. Вип. 194. С. 448–453.

98. Захарченко М. В., Корчинський В. В., Радзімовський Б. К. Структурна скритність таймерних сигналів у системах із кодовим поділом каналів. *Східноєвропейський журнал передових технологій*. 2011. № 2/9 (50). С. 7–9.

99. Корчинський В. В., Кільдішев В. Й., Аль-Файюмі Х., Валігурський Ю. П. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції. *Перспективні напрямки захисту інформації* : матеріали VII міжнар. наук.-практ. конф. (м. Одеса, 30 серп. – 3 верес. 2021 р.). Одеса–Тернопіль : Крок. 2021. С. 31–33.

100. Політанський Р. Л., Готра З. Ю. Дослідження псевдовипадкових послідовностей, генерованих картами хаосу. *Проблеми телекомунікацій*: IV міжнар. наук.-техн. конф. і II студ. наук.-техн. конф. Київ. 2010. С. 127–128.

101. Політанський Л. Ф., Політанський Р. Л., Рождественська М. Г., Гресь О. В. Система передавання даних з використанням псевдовипадкових послідовностей у кодах Хемінга. *Сучасні інформаційні та електронні технології* : тр. XII міжнар. наук.-практ. конф. Одеса, трав. 2011. С. 156.

102. Горохов Ю. С., Бектурсунов Д. Н., Захарченко М. В., Корчинський В. В., Радзімовський Б. К. Зв'язок потужності таймерного коду з числом інформаційних відрізків і твірним елементом Δ . *Вимірювальна та*

обчислювальна техніка в технологічних процесах : матеріали 14-ї міжнар. наук.-техн. конф. (м. Одеса–Затока, 5–10 черв. 2015 р.). Одеса, 2015. С. 240–241.

103. Zakharchenko N. V., Korchinskiy V. V., Radzimovskiy B. K., Bektursunov D. N., Gorokhov Y. S. Assessing the impact of the noise on the throughput communication channel with timing signals. *Eastern European Scientific Journal*. – Düsseldorf : AURIS Kommunikations- und Verlagsgesellschaft mbH, 2015. № 4. С. 209–214.

104. Горохов Ю. С., Корчинський В. В., Рудий Е. М. Метод кодового розділення каналів на основі таймерних сигнальних конструкцій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2016. № 1. С. 208–211.

105. Zakharchenko N., Korchinsky V., Radzimovsky B. Information security of time-controlled signals in confidential communication systems. *Modern problems of radio engineering, telecommunications and computer science* : XI Int. Conf. TCSET (Lviv-Slavske, 21–24 Feb. 2012). Lviv: Publishing House of Lviv Polytechnic, 2012. С. 317.

106. Sha'ameri A. Z., Kanaa A. Robust multiple channel scanning and detection of low probability of intercept (LPI) communication signals. *Defense S&T Technical Bulletin*. 2016. Vol. 9, Iss. 1. P. 1–17.

107. Шпатар П. М., Політанський Р. Л., Гресь О. В., Болонна Є. І. Система передавання даних з шифруванням хаотичними послідовностями. *Обробка сигналів і негаусівських процесів*: IV міжнар. наук.-практ. конф. Черкаси, трав. 2013.

108. Іванюк П. В., Політанський Р. Л. Оцінки чисельних характеристик систем детермінованого хаосу. *Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки*: I Всеукр. наук.-практ. конф. Чернівці, жовт. 2011. С. 107–110.

109. Dedieu H., Kennedy M.P., Hasler M. Chaos Shift Keying. Modulation and Demodulation of a Chaotic Carrier Using Self-synchronizing Chua's Circuits. *IEEE Trans. Circuits and Systems*. 1993. Vol. 40, № 10. P. 634–642.

110. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing Symmetric Operations of Cryptographic Information Encoding. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems* (CPITS II 2021) : CEUR Workshop Proceedings. (Kyiv. October 26, 2021). Kyiv. Ukraine. 2022. P. 182–194.
111. Rudnytskyi V., Korchenko O., Lada N., Ziubina R., Wieclaw L., Hamera L. Cryptographic encoding in modern symmetric and asymmetric encryption. *Procedia Computer Science: 2022 IEEE 26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2022)*. 2022. Vol. 207. P. 54–63.
112. Rudnytskyi V., Lada N., Pochebut M., Melnyk O., Tarasenko Ya. Increasing the cryptographic strength of CET encryption by ensuring the transformation quality of the information block. *13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. (Athens. October 13–15, 2023). Athens, Greece. 2023. P. 1–6.
113. Korchynskyi V. V., Kildishev V. I., Alfaion K. та інші. A method for formation parameters of chaos generators based on hash functions. *Наукові праці ОНАЗ*. Одеса : ОНАЗ, 2020. № 2. С. 65–69.
114. Feldman U., Hasler M., Schwarz W. Communication by Chaotic Signals: the Inverse System Approach. *Int. J. on Circuit Theory and Applications*. 1996. Vol. 24, Iss. 5. P. 551–579.
115. Рябов В.Б., Усик П.В., Ваврів Д.М. Хаотичне маскування без синхронізації. *Радиофизика и радиоастрономия*. 1997. Т. 2, № 4. С. 473–479.
116. Cooper J., McGill K. Probability Methods of Signal and System Analysis. *Cambridge* : Cambridge University Press 1987. 376 p.
117. Захарченко М.В., Мартинова О.М., Горохов Ю.С., Бектурсунов Д.Н., Кріль А.С. Статистичні параметри спотворень таймерних сигнальних конструкцій в каналах моделі Гільберта. *Збірник наукових праць ОНАЗ ім. О.С. Попова*. 2015. № 1. С. 42–47.

118. Haykin S. Communication Systems. 5th ed. Hoboken, NJ : John Wiley & Sons, 2009. 608 p.
119. Lathi B.P., Ding Z. Modern Digital and Analog Communication Systems. *Oxford University Press* : 4th ed. New York. 2009. 964 p.
120. Hsu H.P. Schaum's Outline of Signals and Systems. McGraw-Hill Education : 3rd ed. New York. 2014. 504 p.
121. Zakharchenko N., Korchinsky V., Radzimovsky B. Information security of Time-Controlled Signals in Confidential Communication Systems. *Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012* (Lviv-Slavske, 21–24 February 2012 p. Lviv). Publishing House of Lviv Polytechnic. 2012. P. 317.
122. Schweizer J., Kennedy M.P. Predictive Poincare Control: a Control Theory for Chaotic Systems. *Phys. Rev. E*. 1995. Vol. 52. Iss. 5. P. 4865–4876.
123. Kolumban G., Vizvari R. Nonlinear dynamics and chaotic behavior of sampling phase-locked loops. *Circuits and Systems* : IEEE Trans. 1994. Vol. 41 № 4. P. 333–337.
124. Volkovskii A.R., Young S.C., Tsimring L.S., Rulkov N.F. Multi-User Communication using Chaotic Frequency Modulation. *Proc. Int. Symp. Nonlinear Theory and Its Applications (NOLTA'01)*. Miyagi. 2001. P. 561–564.
125. Pecora L.M., Carroll T.L. Synchronization in Chaotic Systems. *Phys. Rev. Lett.* 1990. Vol. 64, № 8. P. 821–824.
126. Kennedy M.P., Columban G. Chaotic Modulation for Robust Digital Communications over Multipath Channels. *Int. J. Bifurcation Chaos*. 2000. Vol. 10, № 4. P. 695–719.
127. Голдвассер С., Мікалі С. Ймовірнісне шифрування та як грати в ментальний покер, зберігаючи в секреті всю часткову інформацію. *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*. 1982. С. 365–377.
128. Молдован А. Гомофонний шифр. Теоретичні основи та практичне застосування. *Видавництво технічної літератури*. Київ. 2002. 250 с.

129. Мальцев Г. Н., Чернявський Є. В. Шляхи підвищення достовірності передачі повідомлень в умовах односторонньої радіопередачі. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2021. №1. С. 56–72.

130. Bohme F., Feldman U., Schwarz W., Bauer A. Information transmission by chaotizing. Workshop on Nonlinear Dynamics of Electronic Systems (NDES'94) : Proc. 2nd Int. Krakov. 1994. P. 163–168.

131. Корчинський В.В., Кільдішев В.Й., Онищук В.В., Аль-Файюмі Х. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційних системах веб-сервісів. *Науковий журнал «Інфокомунікаційні та комп'ютерні технології»*. Відкритий міжнародний університет розвитку людини «Україна». Київ. 2021. № 2 (02). С. 195–201.

132. Корчинський В.В., Аль-Файюмі Х. Методи застосування динамічного хаосу в системах захисту інформації. *Забезпечення кібероборони держави*: зб. матеріалів IV наук.-практ. Вебінару. НУОУ. (м. Київ, 10 листопада 2023 р.). Київ. 2023. С. 81–83.

133. Blahut R. Theory and Practice of Error Control Codes. *Addison-Wesley* 1983. 576 p.

134. Корчинський В.В., Казакова Н.Ф., Трінтіна Н.А. Аналіз статистики помилок у системах передавання зі змінними параметрами. *Наукові праці ОНАЗ ім. О. С. Попова*. 2002. № 1. С. 85–93.

135. Hordiichuk V., Korchynskyi V., Kildishev V., Molodetskyi B., Staikutsa S., Alfaiomi K. Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare. *Telecommunications and Computer Engineering (TCSET) : 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics*. Lviv. 2024. P. 1–4. doi:10.1109/TCSET64720.2024.10755658.

136. Onyshchuk V., Kildishev V., Korchynskyi V. and Khaled Alfaiomi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services. *Telecommunications and Computer Engineering (TCSET): Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics*. (Ukraine February 22-26, 2022). Lviv-Slavske. 2022. P. 331-334.

137. Korchynskiy V., Kildishev V., Golev D. Increase of transmission security based on timer signal construction. 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 10–14 September 2018, Odessa. P. 1–4. doi:10.1109/UkrMiCo43733.2018.9047554.

138. Кільдішев В.Й., Корчинський В.В., Онищук В.В., Аль-Файюми Х. Підвищення захищеності користувацьких даних веб-серверів шляхом впровадження гомоморфного шифрування. *Матеріали 75-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів*, тези доповідей. Одеса: ОНАЗ, 2020. С. 132–133.

139. Korchynskiy V., Kildishev V., Berdnikov O., Valihurskiy Y., Polyshchuk K. The Methods of Forming Random Sequences Based on the Dynamic Chaos. «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах»: VIII Міжнародна наук.-практ. конф. (м. Чернівці, 3–5 жовтня 2019 р.). Чернівці, 2019. С. 26-29.

140. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Губін А.В. Системи радіозв'язку із шумоподібними таймерними сигналами. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів*, тези доповідей. Одеса: ОНАЗ, 2018. С. 134-136.

141. Корчинський В.В., Кільдішев В.Й., Голев Д.В. Прихованість та завадостійкість передачі інформації на основі випадкового таймерного кодування. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів*, тези доповідей. Одеса: ОНАЗ, 2018. С. 133-134.

142. Zakharchenko M., Korchynskiy V., Kildishev V. Integrated Methods of Information Security in Telecommunication Systems. 2017 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017). Odessa, 11–15 Sept. 2017. V.1. P. 78-81.

143. Korchynskiy V., Kildishev V., Riabukha O., Berdnikov O. The generating random sequences with the increased cryptographic strength. *Informatics, Automatics and Control Systems*. 2020. No. 1. P. 20-23. – DOI: 10.35784/iapgos.916

144. Шпатар П.М., Політанський Р.Л., Гресь О.В., Болонна Є.І. Система передавання даних з шифруванням хаотичними послідовностями. *Обробка сигналів і негаусівських процесів* : IV Міжнародна науково-практична конференція. Черкаси, травень 2013.

145. Горохов С.М., Захарченко М.В., Корчинський В.В. Критерії ефективності прихованих методів передачі. *Цифрові технології*. Одеська нац. академія зв'язку ім. О.С. Попова. Одеса. 2012. Вип. 12. С. 147–150.

146. Голевич О.Б. Спосіб детектування хаотичних сигналів в умовах дії завад. *Вимірювальна та обчислювальна техніка в технологічних процесах* : 14-а Міжнародна науково-технічна конференція (ВОТТП_14_2015). м. Одеса, 5–9 червня 2015.

147. Голевич О.Б., Пивовар О.С. Застосування прямохаотичних надширокосмугових технологій у телекомунікаційних системах. Міжнародна науково-практична конференція «Інформаційні процеси та технології». Севастополь. 22–26 квітня 2013. С. 109.

148. Голевич О.Б. Дослідження використання хаотичних коливань для телекомунікацій інформаційних сигналів. 7-а Міжнародна науково-технічна конференція АПКТ-2013. (м. Хмельницький, 23 травня 2013). Хмельницький. С. 71.

149. Галюк С.Д., Політанський Л.Ф., Гресь О.В., Політанський Р.Л. Система передавання даних з використанням генераторів хаосу. *Радиотехника*. 2011. № 164. С. 66–71.

150. Корчинський В., Мар'ян М., Богданюк І., Аль-Файюмі Х. Метод захисту інформації від несанкціонованого доступу на основі динамічного хаосу. *Scientific Collection «InterConf»*. 2024. № 194. С. 448–453.

151. Корчинський В.В., Аль-Файюмі Х. Методи застосування динамічного хаосу в системах захисту інформації. *Забезпечення кібероборони держави* : збірник матеріалів IV науково-практичного вебінару. НУОУ. (м. Київ, 10 лист. 2023 р.) Київ. 2023. С 81–83.

152. Радзімовський Б. К. Синтез телекомунікаційних сигналів на основі хаотичних коливань : автореф. дис. канд. техн. наук : 05.12.13. Одес. нац. акад. зв'язку ім. О.С. Попова. Одеса, 2014. 120 с.

153. Захарченко М. В., Корчинський В. В., Радзімовський Б. К., Кільдішев В. Й. Підвищення скритності передачі конфіденційної інформації на базі хаотичних сигналів та таймерних сигнальних конструкцій. *Східноєвропейський журнал передових технологій*. 2012. № 3/9 (57). С. 45-49. DOI: <https://doi.org/10.15587/1729-4061.2012.4168>.

154. Корчинський В. В., Кільдішев В. Й., Осадчук К. О., Бердніков О. М. Дослідження енергетичної прихованості шумоподібних таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ». Серія : Нові рішення в сучасних технологіях*. 2018. № 42 (1214). С. 126-130. DOI: <https://doi.org/10.20998/2413-4295.2018.12.01>.

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Сталий розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б. В. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. Одеса : ДУ «ІРЕЕД НАНУ», 2024. 543 с.
2. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaiomi Kh. Method of information protection based on the integration of probabilistic encryption and noise immune coding. *Radioelectronic and Computer Systems*. 2023. Vol. 4, No. 13. P. 184-196.
3. Корчинський В. В., Кільдішев В. Й., Онищук В. В., Аль-Файюми Халед. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційних системах веб-сервісів. *Інфокомунікаційні та комп'ютерні технології*. 2021. № 2 (02). С. 195–201.
4. Korchynskyi V. V., Kildishev V. I., Alfaion K. та інші. A method for formation parameters of chaos generators based on hash functions. *Наукові праці ОНАЗ*. 2020. № 2. P. 65-69.
5. Korchynskyi V., Kildishev V., Riabukha O., Berdnikov O. The generating random sequences with the increased cryptographic strength. *Informatics, Automatics and Control Systems*. 2020. No. 1. P. 20-23.
6. Hordiichuk V., Shyshatskyi A., Korchynskyi V., Kildishev V. Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems. *Journal of Physics: Conference Series*. 2021. Vol. 1839. P. 1-10.
7. Korchynskyi V. V., Kildishev V. I., Berdnikov A. M., Smazhenko K. O. Increase of stealth transmission based on timer signals and linear frequency modulation. *Наукові праці ОНАЗ ім. О. С. Попова*. 2020. № 1. P. 53-57.
8. Korchynskyi V. V., Kildishev V. I., Holey D. V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding. *Radio Electronics, Computer Science, Control*. 2019. No. 3 (50). P. 108-116.

9. Korchynskiy V. V., Kildishev V. I., Berdnikov A. M., Bielova I. V. Methods for generating noise-like timer signals based on pseudo-random tuning of the operating frequency. *Наукові праці ОНАЗ ім. О. С. Попова*. 2019. № 2. С. 98-103.

10. 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. Р. 93-97.

11. Корчинський В. В., Кільдішев В. Й., Осадчук К. О., Бердніков О. М. Дослідження енергетичної прихованості шумоподібних таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ». Серія : Нові рішення в сучасних технологіях*. 2018. № 42 (1214). С. 126-130.

12. Korchynskiy V. V., Kildishev V. I., Holey D. V., Berdnikov A. M. Research methods of increasing the security of information transfer based on timer signals. *Наукові праці ОНАЗ ім. О. С. Попова*. 2018. № 2. С. 109-115.

13. Корчинський В. В., Кільдішев В. Й., Бердніков О. М., Осадчук К. О. Підвищення захищеності системи зв'язку з таймерними сигнальними конструкціями та псевдовипадковою перебудовою робочої частоти. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 2. С. 179-182.

14. Korchynskii V. V., Kildishev V. I., Berdnikov A. M. Methods for assessing the security of communication systems for special purposes. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 2. Р. 101-107.

15. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Толкачов А. В. Ефективність двосимвольних ансамблів у симплексних системах на базі коригувальних таймерних сигнальних конструкцій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 1. С. 215-218.

16. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Осадчук К. О. Інформаційні параметри кодів Сліп'яна з компенсацією надмірності таймерними сигналами. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 1. С. 14-20.

17. Korchynskii V. V., Osadchuk E. A., Kildishev V. I. Method of multiplexing of timer signal structures based on OFDM technology. *Вісник Національного університету «Львівська політехніка»*. 2017. № 2. Р. 41-44.

18. Стайкуца С. В., Кільдішев В. Й. Ідентичність об'єктів інформаційної мережі як елемент моделі кібербезпеки. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2016. № 2. С. 185-189.

19. Захарченко М. В., Корчинський В. В., Радзімовський Б. К., Кільдішев В. Й. Підвищення скритності передачі конфіденційної інформації на базі хаотичних сигналів та таймерних сигнальних конструкцій. *Східноєвропейський журнал передових технологій*. 2012. № 3/9 (57). С. 45-49.

20. Корчинський В. В., Кільдішев В. Й., Хомич С. В., Белова Ю. В. Ефективність j -кратного повторення надлишкових таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ»*. 2012. Вип. 26. С. 88-95.

21. Захарченко М. В., Кільдішев В. Й., Белова Ю. В., Хомич С. В. Вплив корельованих завад на пропускну здатність безперервного каналу зв'язку. *Вісник НТУ «ХПІ». Серія : Нові рішення у сучасних технологіях*. 2012. Вип. 33. С. 62-68.

22. Захарченко М. В., Кільдішев В. Й., Хомич С. В., Пришляк О. Г. Компенсація надлишковості в блокових коректуючих кодах за рахунок таймерних сигналів. *Вісник Хмельницького національного університету*. 2011. Вип. 2. С. 175-181.

23. Шевцов Ю. С., Кононович В. Г., Кільдішев В. Й. Модель спільного використання системи виявлення і обробки атак із системою постійного аудиту інформаційної безпеки. *Вісник Східноукраїнського національного університету ім. В. Даля*. 2010. № 9 (151), ч. 1. С. 52-58.

24. Hordiichuk V., Korchynskyi V., Kildishev V., Molodetskyi B., Staikutsa S., Alfaiomi K. Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare. *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv, Ukraine, 2024. P. 1-4.

25. Кільдішев В.Й. Система оцінок захищеності методів захисту інформації в умовах РЕБ. *Забезпечення кібероборони держави : збірник матеріалів IV наук.-практ. вебінару* (м. Київ, 10 листопада 2023 р.). Київ: НУОУ, 2023. С. 65-68.

26. Onyshchuk V., Kildishev V., Korchynskyi V., Alfaioni K. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services. *Proc. 16th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 22–26 Feb. 2022. P. 331-334.

27. Hordiichuk V., Korchynskyi V., Kildishev V., Zakharchenko M. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods. *2022 IEEE 2nd Ukrainian Microwave Week (UkrMW)*. Kyiv, 14-18 Nov. 2022. P. 331-334.

28. Корчинський В.В., Кільдішев В.Й., Аль-Файюми Х., Валігурський Ю.П. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції. *Перспективні напрямки захисту інформації: матеріали VII міжнар. наук.-практ. конф.* (м. Одеса, 30 серпня – 3 вересня 2021 р.). Одеса–Тернопіль: Крок, 2021. С. 31-33.

29. Korchynskyi V., Kildishev V., Golev D. Increase of Transmission Security Based on Timer Signal Construction. *2018 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. Odessa, 10–14 Sept. 2018. P. 1-4.

30. Корчинський В.В., Кільдішев В.Й., Онищук В.В., Аль-Файюми Х. Підвищення захищеності користувацьких даних веб-серверів шляхом впровадження гомоморфного шифрування. *Матеріали 75-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей*. Одеса: ОНАЗ, 2020. С. 132–133.

31. Korchynskyi V., Kildishev V., Berdnikov O., Valihurskyi Y., Polyshchuk K. The Methods of Forming Random Sequences Based on the Dynamic Chaos. *VIII Міжнародна наук.-практ. конф. «Фізико-технологічні проблеми передавання,*

оброблення та зберігання інформації в інфокомунікаційних системах» (м. Чернівці, 3–5 жовтня 2019 р.). Чернівці, 2019. С. 26-29.

32. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Губін А.В. Системи радіозв'язку із шумоподібними таймерними сигналами. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів*, тези доповідей. Одеса: ОНАЗ, 2018. С. 134-136.

33. Корчинський В.В., Кільдішев В.Й., Голев Д.В. Прихованість та завадостійкість передачі інформації на основі випадкового таймерного кодування. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів* : тези доповідей. Одеса: ОНАЗ, 2018. С. 133-134.

34. Zakharchenko M., Korchynskyi V., Kildishev V. Integrated Methods of Information Security in Telecommunication Systems. *2017 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017)*. Odessa, 11–15 Sept. 2017. V.1. P. 78-81.

35. Корчинський В.В., Кільдішев В.Й. Захищеність систем зв'язку спеціального призначення. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (13-15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 18-19.

36. Корчинський В.В., Кільдішев В.Й. Підвищення прихованості передачі в системі зв'язку з кодовим розділенням каналів на основі динамічного хаосу. *XIX Міжнар. наук.-практ. конф. «Безпека інформації у інформаційно-телекомунікаційних системах»* (м. Буча, 25–26 травня 2017 р.). Буча: Держспецзв'язок, 2017. С. 48.

37. Корчинський В. В., Кільдішев В. Й., Бердніков О. М. Методи розширення спектру таймерних сигналів на основі псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали IV Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 57-59.

38. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Валігурський Ю.П. Метод порівняльного аналізу генераторів псевдовипадкових чисел.

Перспективні напрями захисту інформації: матеріали IV Всеукр. наук.-практ. конф. (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 46-48.

39. Корчинський В.В., Кільдішев В.Й., Осадчук К.О., Русаловська О.А. Підвищення захищеності передачі інформації на основі таймерних сигнальних конструкцій та технології OFDM. *Перспективні напрями захисту інформації : матеріали III Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 39-42.

40. Кільдішев В.Й., Бердніков О.М., Степанов В.О. Підвищення захищеності системи зв'язку з ППРЧ на основі таймерних сигнальних конструкцій. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (м. Черкаси, 13–15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 17-18.

41. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Русаловська О.А. Спектральні методи захисту інформації на основі таймерних сигналів та псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали III Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 36–39.

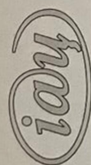
42. Корчинський В.В., Кільдішев В.Й., Бердніков О.М. Методи підвищення захищеності систем зв'язку на основі таймерних сигналів. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей.* Одеса: ОНАЗ, 2017. С. 114-117.

43. Корчинський В.В., Кільдішев В.Й., Валігурський Ю.П., Поліщук К.В. Підвищення ефективності потокового шифрування в радіомережах на основі динамічного хаосу. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів : тези доповідей.* Одеса: ОНАЗ, 2017. С. 117-118.

44. Захарченко М.В., Корчинський В.В., Кільдішев В.Й. Про доцільність застосування зворотного зв'язку в системах передачі даних. *Матеріали 64-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів* (м. Одеса, 1–4 грудня 2009 р.). Одеса: ОНАЗ, 2009. С. 78-80.

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ



ОДЕСЬКА ОБЛАСНА РАДА
КОМУНАЛЬНЕ ПІДПРИЄМСТВО
«ОБЛАСНИЙ ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ЦЕНТР»
(КП ОІАЦ)
пр-т. Шевченка, 4, м. Одеса, 65032, тел.: 718-93-47, факс: 42-98-12, e-mail: iac@od.gov.ua
web: <https://iac.od.gov.ua>, код ЄДРПОУ 25053256

АКТ ВПРОВАДЖЕННЯ

розробок дисертаційної роботи «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій»

на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – системи захисту інформації
КІЛЬДІШЕВА ВІТАЛІЯ ЙОСИПОВИЧА

м. Одеса

« ____ » ____ 2025 р.

Ми, що нижче підписалися, представники комунального підприємства «Обласний інформаційно-аналітичний центр», розглянувши результати дисертаційної роботи, підтверджуємо їх практичну значущість та можливість використання у сфері забезпечення інформаційної безпеки.

У процесі впровадження використано такі науково-технічні розробки:

- система багаторівневого захисту інформації, побудована на інтеграції стохастичного шифрування із завадостійким кодуванням, декореляцією помилок і таймерним кодуванням, у якій додатково реалізовані механізми захисту від несанкціонованого доступу;
- алгоритм стохастичного шифрування, що забезпечує формування шифrogramи шляхом добору випадкових кодових комбінацій з урахуванням імовірнісного розподілу появи символів у відкритому тексті;
- методики, що спрямовані на підвищення криптостійкості, енергетичної та структурної прихованості сигнально-кодових конструкцій у захищених каналах зв'язку;
- умови забезпечення енергетичної прихованості для методів розширення спектра – псевдовипадкової побудови робочої частоти, прямого розширення спектра за допомогою псевдовипадкових послідовностей та лінійної частотної модуляції, що сприяють підвищенню захищеності каналів зв'язку в умовах радіоселективного впливу;

Отримані результати впроваджені у діяльність комунального підприємства «Обласний інформаційно-аналітичний центр» у частині підвищення рівня інформаційної безпеки корпоративних інформаційно-комунікаційних систем.

Директор

Акім КОЄВ



Відповідальний виконавець,
заступник директора
з IT та розвитку

Дмитро ГОНЧАРУК

ПРОЄКТУВАННЯ, МОНТАЖ, ОБСЛУГОВУВАННЯ

- систем охорони-пожежної сигналізації;
- систем інтелектуального контролю вхідних дверей;
- ефірного та супутникового телебачення;
- телефонних, комп'ютерних мереж та мні АТС;
- систем відеонагляду, аудіо-відео домоніторингу;
- систем охорони на складі, апаратури напруги;
- систем блокування дверей та замків;
- енергетичних мереж, альтернативних джерел енергії.

Ліцензія ДПБ України АЕ № 94443 від 26 лютого 2015 р.

ПП "АРДО"
 Р/Р 26001054347471
 в ПАТ "ТРИАТБАНК"
 МФО328704, Код ЄДРР0924532240
 ІПН 24532245538
 сф.до плат. ПДВ 2309520



"АРДО"
пришвидчене підприємство

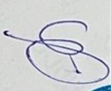
АКТ ПРО ВПРОВАДЖЕННЯ
результатів дисертаційної роботи «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій»
на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації
КІЛЬДІШЕВА ВІТАЛІЯ ЙОСИПОВИЧА

Комісія у складі: виконуючого директора ПП «АРДО» Бердікова Олександра Михайловича, Головного інженера ПП «АРДО» Кожевнікова Євгена Володимировича.

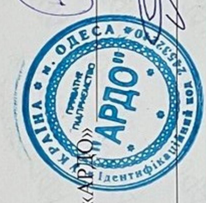
На підставі аналізу результатів дисертаційної роботи «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» підтверджуємо, що отримані наукові та практичні напрацювання можуть бути впроваджені у діяльність підприємства ПП «АРДО».

Особливу практичну цінність становлять такі результати:

- 1) запропонований метод синтезу шумоподібних таймерних сигналів із використанням лінійної частотної модуляції, що забезпечує підвищення енергетичної та структурної прихованості;
- 2) методика формування початкових параметрів генераторів хаосу на основі генування символів користувачького паролю з подальшим перетворенням геш-коду у відповідний діапазон числових значень;
- 3) методи, що спрямовані на підвищення криптостійкості, енергетичної та структурної прихованості сигнально-кодових конструкцій у захищених каналах зв'язку.

В.о. директора ПП «АРДО» 
 Олександр БЕРДІКОВ

Головний інженер 
 Євген КОЖЕВНІКОВ



65000, Україна, Одеса, вул. Рокоссовського, 3
 Зв'язок: 77-27-74, 77-27-74
 www.ar-do.odessa.ua
 E-mail: office@ar-do.odessa.ua

ЗАТВЕРДЖУЮ
 Проректор-завідувач роботи
 Державного університету інтелектуальних
 технологій і зв'язку
 проф. д-р. н. держ. управ.
 С.К. Халжирадєва
 «15» вересня 2025 року

Ліцензія ДПБ України АЕ № 94443 від 26 лютого 2015 р.

АКТ
впровадження результатів дисертаційної роботи
КІЛЬДІШЕВА ВІТАЛІЯ ЙОСИПОВИЧА
на тему: «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій»

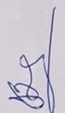
Комісія в складі:

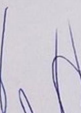
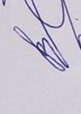
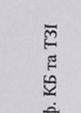
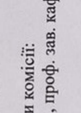
голова – декан факультету ІТК д.т.н. проф. Васіліу Є.В.;

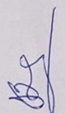
члени комісії: д.т.н. проф. завідувач каф. КБ та ТЗІ Корчинський В.В., к.ф.н. доц. каф. КБ та ТЗІ Стайкуца В.В., стар. викладач Рябуха О.М., секретар каф. КБ та ТЗІ Дунаєва В.В.

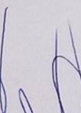
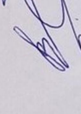
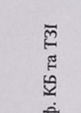
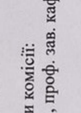
склада цей акт про те, що результати дисертаційної роботи здобувача кафедри кібербезпеки та технічного захисту інформації Кільдішева Віталія Йосиповича на тему «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» впроваджені у навчальний процес на кафедрі кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку.

Матеріали дисертації увійшли до складу дисциплін «Методи та засоби захисту інформації» і «Моніторинг та аудит інформаційно-комунікаційних систем», що викладаються на факультеті інформаційних технологій та кібербезпеки студентам четвертого курсу першого (бакалаврського) рівня, які навчаються за напрямом підготовки спеціальності 125 Кібербезпека та захист інформації.

Голова комісії:
 Декан факультету ІТК ДУІТЗ,
 д.т.н., проф. 
 Васіліу Є.В.

Члени комісії:
 д.т.н., проф. зав. каф. КБ та ТЗІ 
 Корчинський В.В.
 к.ф.н., доц. каф. КБ та ТЗІ 
 Стайкуца В.В.
 к.т.н., стар. викл. каф. КБ та ТЗІ 
 Рябуха О.М.
 секретар каф. КБ та ТЗІ 
 Дунаєва В.В.

Голова комісії:
 Декан факультету ІТК ДУІТЗ,
 д.т.н., проф. 
 Васіліу Є.В.

Члени комісії:
 д.т.н., проф. зав. каф. КБ та ТЗІ 
 Корчинський В.В.
 к.ф.н., доц. каф. КБ та ТЗІ 
 Стайкуца В.В.
 к.т.н., стар. викл. каф. КБ та ТЗІ 
 Рябуха О.М.
 секретар каф. КБ та ТЗІ 
 Дунаєва В.В.