

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

Кваліфікаційна наукова праця
На правах рукопису

СТЕПАНОВ ВАДИМ ОЛЕКСАНДРОВИЧ

УДК 004.056.53:621.391.7

ДИСЕРТАЦІЯ

**ПІДВИЩЕННЯ ПРИХОВАНOSTІ ПЕРЕДАВАННЯ ШИРОКОСМУГОВИХ
ТАЙМЕРНИХ СИГНАЛІВ НА ОСНОВІ ПСЕВДОВИПАДКОВОГО
ПЕРЕСКОКУ РОБОЧОЇ ЧАСТОТИ**

Спеціальність 125 Кібербезпека
Галузь знань 12 Інформаційні технології
Подається на здобуття ступеня
доктора філософії

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

_____ Степанов Вадим Олександрович
(підпис)

Науковий керівник: КОРЧИНСЬКИЙ Володимир Вікторович,
доктор технічних наук, професор

Одеса – 2026

АНОТАЦІЯ

Степанов В. О. Підвищення прихованості передавання широкосмугових таймерних сигналів на основі псевдовипадкового перескоку робочої частоти – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека. – Державний університет інтелектуальних технологій і зв'язку, Одеса, 2026.

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано нове вирішення актуального наукового завдання, спрямованого на підвищення прихованості передавання інформації в системах радіозв'язку, що функціонують в умовах радіоелектронного протиборства. Запропоновані рішення базуються на інтеграції таймерних сигнальних конструкцій із методами псевдовипадкового перескоку робочих частот для формування комбінованих шумоподібних сигналів із підвищеною структурною невизначеністю. При цьому вирішено задачу підвищення структурної та енергетичної прихованості сигнально-кодкових конструкцій шляхом поєднання часового, частотного та кодового розширення спектра, що забезпечує зниження ймовірності виявлення, класифікації та перехоплення сигналів у нестационарних умовах функціонування каналів радіозв'язку.

Метою дисертаційної роботи є підвищення рівня захисту інформації в інформаційно-комунікаційних системах шляхом розроблення методів формування прихованих широкосмугових сигналів на основі інтеграції таймерних сигнальних конструкцій, псевдовипадкового перескоку робочих частот, що забезпечують зниження ймовірності виявлення, перехоплення та структурного аналізу переданої інформації в умовах радіоелектронної протидії.

Об'єкт дослідження – процеси захисту інформації під час її передавання в інформаційно-комунікаційних системах в умовах радіоелектронної протидії та інформаційно-технічних впливів.

Предмет дослідження – методи підвищення прихованості передавання інформації на основі формування та інтеграції таймерних сигнальних конструкцій,

технологій псевдовипадкового перескоку робочих частот в інформаційно-комунікаційних системах.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок роботи з науковими програмами та темами, наведено наукову новизну і практичну цінність отриманих результатів, визначено особистий внесок здобувача. Подано відомості щодо апробації результатів дослідження та публікацій автора.

У *першому розділі* дисертаційної роботи проведено аналіз умов функціонування систем радіозв'язку в умовах радіоелектронної протидії, а також розглянуто основні методи захисту інформації від несанкціонованого доступу шляхом підвищення прихованості та завадостійкості передавання сигнально-кодових конструкцій. Встановлено, що сучасне радіоелектронне середовище характеризується високим рівнем активних, пасивних та імітаційних завад, а також широким застосуванням засобів радіорозвідки, що суттєво ускладнює забезпечення стійкого та прихованого передавання інформації.

Проаналізовано вплив радіоелектронної протидії на ключові параметри каналів зв'язку, зокрема відношення сигнал/шум, синхронізацію, ймовірність помилок та пропускну здатність. Показано, що в умовах інтенсивного завадового впливу відбувається комплексна деградація характеристик радіоканалів, що обмежує ефективність класичних методів передавання інформації.

Розглянуто основні методи до підвищення прихованості та завадостійкості, включаючи технології розширення спектра, псевдовипадкового перескоку робочої частоти, а також використання широкосмугових сигналів. Встановлено, що існуючі методи мають обмеження щодо забезпечення одночасно високого рівня прихованості та стійкості до сучасних засобів радіорозвідки.

Проаналізовано можливості застосування таймерних сигнальних конструкцій як перспективної основи для формування прихованих каналів зв'язку, що забезпечують реалізацію додаткового часового ступеня свободи під час кодування інформації.

На основі проведеного аналізу обґрунтовано доцільність подальшого розвитку комбінованих методів передавання інформації, що інтегрують таймерні сигнальні конструкції та механізми псевдовипадкового перескоку робочих частот, з метою підвищення структурної невизначеності та прихованості сигналів, а також зменшення ймовірності їх виявлення, класифікації та перехоплення в умовах радіоелектронної протидії.

У другому розділі досліджено теоретичні основи методів розширення спектра та їх роль у забезпеченні захисту інформації в системах радіозв'язку. Проведено аналіз технологій прямого розширення спектра псевдовипадковими послідовностями (ПРС-ПВП) та псевдовипадкового перескоку робочої частоти (ППРЧ), визначено їх переваги та обмеження щодо забезпечення завадостійкості, енергетичної та структурної прихованості передавання інформації.

Розроблено та проаналізовано математичні моделі сигналів із розширеним спектром, що дозволило формалізувати процеси кодового й частотного розосередження енергії, визначити параметри обробного виграшу та оцінити вплив ширини спектра на енергетичну прихованість і стійкість до навмисних завад. Показано особливості функціонування систем на основі ПРС-ПВП та ППРЧ, а також встановлено обмеження класичних методів, пов'язані з наявністю кореляційних ознак, залежністю від синхронізації та частковою структурною повторюваністю сигналів.

Досліджено комбіновані методи розширення спектра, що інтегрують механізми кодового та частотного розширення. Показано, що поєднання ПРС-ПВП і ППРЧ забезпечує підвищення обробного виграшу, зменшення спектральної густини потужності, збільшення живучості каналу зв'язку та зниження ймовірності енергетичного й структурного виявлення сигналів.

Встановлено, що застосування таймерних сигнальних конструкцій (ТСК) забезпечує додатковий ступінь структурної невизначеності сигналів за рахунок використання часових параметрів для кодування інформації та збільшення кількості можливих сигнально-кодових реалізацій. Показано, що інтеграція ТСК з

методами ПРС-ПВП та ППРЧ дозволяє формувати комбіновані шумоподібні сигнали з підвищеною прихованістю та стійкістю до виявлення.

Отримані результати сформували теоретичне підґрунтя для подальшого розроблення методів підвищення прихованості передавання інформації на основі інтеграції таймерних сигнальних конструкцій із псевдовипадковим перескоком робочих частот, що розглядається у наступному розділі дисертаційної роботи.

У *третьому розділі* досліджено теоретичні засади формування таймерних сигнальних конструкцій як основи для захисту інформації шляхом підвищення структурної прихованості сигнально-кодових конструкцій в системах радіозв'язку. Проведено аналіз принципів побудови позиційних і непозиційних сигналів та встановлено, що таймерні сигнальні конструкції належать до класу непозиційних сигналів, у яких інформаційне навантаження визначається сукупністю часових інтервалів між значущими моментами модуляції. Показано, що такий підхід забезпечує додатковий часовий ступінь свободи кодування та суттєво розширює множину можливих сигнальних реалізацій.

Розроблено математичні моделі таймерних сигнальних конструкцій та досліджено закономірності їх формування. Встановлено, що кількість можливих сигнальних реалізацій визначається параметрами таймерного кодування та зростає за комбінаторним законом, забезпечуючи значне збільшення ансамблю сигналів порівняно з класичними позиційними кодами.

Виконано аналіз спектральних і кореляційних властивостей таймерних сигналів. Показано, що нерегулярна структура часових інтервалів формує шумоподібний спектр зі зменшеними дискретними складовими, що сприяє підвищенню енергетичної прихованості та ускладнює спектральне виявлення сигналів засобами радіоелектронної розвідки. Досліджено автокореляційні та взаємкореляційні характеристики таймерних сигналів і встановлено, що їх структура дозволяє формувати широкий ансамбль шумоподібних сигнально-кодових конструкцій.

Досліджено особливості кореляційного приймання таймерних сигналів. Показано, що використання класичних позиційних кореляційних приймачів не

забезпечує коректного відновлення структури таймерних сигнальних конструкцій через відсутність фіксованого розташування інформаційних елементів у часовій області, що призводить до виникнення локальних максимумів кореляційної функції та часткових кореляційних збігів.

Доведено, що застосування таймерних сигнальних конструкцій забезпечує формування додаткової часової невизначеності та підвищує структурну прихованість сигналів ще до використання класичних методів розширення спектра. Отримані результати створюють теоретичне підґрунтя для подальшого синтезу комбінованих методів захисту інформації на основі інтеграції таймерних сигналів із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот, що розглядається у наступному розділі дисертаційної роботи.

У *четвертому розділі* дисертаційної роботи розроблено та досліджено методи підвищення прихованості передавання інформації на основі інтеграції таймерних сигнальних конструкцій із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот. Проведено аналіз параметрів таймерних сигналів і встановлено, що їх формування базується на міжімпульсних інтервалах. Показано, що збільшення зазначених параметрів побудови сигнальних конструкцій приводить до експоненційного зростання кількості можливих сигнальних реалізацій та безпосередньо підвищує структурну прихованість сигналів.

Виконано порівняльний аналіз спектральної та енергетичної ефективності таймерних і позиційних сигналів. Встановлено, що таймерні сигнальні конструкції характеризуються вищою частотною ефективністю завдяки більшій інформаційній насиченості часової структури, що підтвердило доцільність їх використання як основи для формування шумоподібних сигналів у системах захищеного радіозв'язку.

Розроблено методи розширення спектра таймерних сигналів на основі прямого розширення спектра та псевдовипадкового перескоку робочих частот. Для технології ППРЧ сформовано алгоритми швидкої, повільної та багатоканальної перебудови частоти, адаптовані до непозиційної структури таймерних сигнальних

конструкцій. Показано, що запропонований підхід забезпечує інтеграцію частотного розширення спектра без втрати властивостей таймерного кодування та дозволяє формувати комбіновані шумоподібні сигнали з підвищеним рівнем прихованості.

Досліджено закономірності формування структурної прихованості комбінованих сигналів та встановлено, що вона визначається сукупною дією часової, кодової та частотної невизначеності. Показано, що внесок псевдовипадкового перескоку робочих частот залежить не лише від кількості доступних частотних позицій, а й від кількості частотних перебудов у межах сигналу, що формує множину можливих частотних траєкторій та додатково ускладнює його реконструкцію.

Проведений аналіз залежності структурної прихованості від параметрів таймерних сигналів, ПРС-ПВП та ППРЧ підтвердив її експоненційне зростання зі збільшенням бази комбінованого сигналу. Встановлено, що зростання інтегральної бази сигналу супроводжується підвищенням ентропії, шумоподібності та завадозахищеності, ускладнюючи виявлення, класифікацію та відновлення сигналу сторонніми засобами спостереження. Разом із тим показано, що надмірне розширення спектра підвищує вимоги до синхронізації та технічної реалізації системи зв'язку, що обґрунтовує необхідність адаптивного вибору параметрів комбінованих методів залежно від умов функціонування системи.

У висновках дисертаційної роботи узагальнено результати проведених досліджень, сформульовано основні наукові положення та практичні рекомендації, що впливають із отриманих результатів, а також наведено кількісні оцінки ефективності запропонованих методів і рішень в умовах їх застосування.

У додатках до дисертаційної роботи наведено матеріали щодо впровадження отриманих результатів, а також подано перелік наукових публікацій та апробацій автора, виконаних за тематикою дисертаційного дослідження.

Ключові слова: захист інформації, прихованість передавання інформації, інформаційно-комунікаційні системи, системи радіозв'язку, таймерні сигнальні конструкції, псевдовипадкове перескоку робочих частот, шумоподібні сигнали,

розширення спектра, псевдовипадкові послідовності, структурна прихованість, автокореляція, взаємна кореляція, радіоелектронна протидія, завадозахищеність, сигнально-кодові конструкції, непозиційні сигнали, інформаційна безпека.

SUMMARY

Stepanov V. O. Increasing the secrecy of transmission of broadband timing signals based on pseudo-random hopping of the operating frequency – Qualifying scientific work on the rights of the manuscript.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the specialty 125 "Cyber Security" – State University of Intelligent Technologies and Telecommunications, Odesa, 2026.

The dissertation provides a theoretical generalization and proposes a new solution to an urgent scientific problem aimed at enhancing the concealment of information transmission in radio communication systems operating under conditions of electronic warfare. The proposed solutions are based on the integration of timer signal structures with frequency hopping spread spectrum techniques to generate combined noise-like signals with increased structural uncertainty. In particular, the problem of improving the structural and energy concealment of signal-code structures is solved by combining temporal, frequency, and code spectrum spreading, which reduces the probability of signal detection, classification, and interception under non-stationary operating conditions of radio communication channels.

The aim of the dissertation is to improve the level of information protection in information and communication systems by developing methods for generating covert broadband signals based on the integration of timer signal structures and frequency hopping spread spectrum techniques, which ensure a reduced probability of detection, interception, and structural analysis of transmitted information under conditions of electronic countermeasures.

The object of the research is the processes of information protection during its transmission in information and communication systems under conditions of electronic countermeasures and information-technical impacts.

The subject of the research is methods for improving the concealment of information transmission based on the generation and integration of timer signal structures and frequency hopping spread spectrum technologies in information and communication systems.

The introduction substantiates the relevance of the dissertation topic, formulates the research objective and the scientific and applied tasks required to achieve it, demonstrates the relationship of the study with scientific programs and research projects, presents the scientific novelty and practical significance of the obtained results, and identifies the personal contribution of the applicant. Information concerning the approbation of the research results and the author's publications is also provided.

The first chapter of the dissertation analyzes the specific features of the functioning of radio communication systems under conditions of electronic countermeasures and examines the main methods of information protection against unauthorized access by enhancing the concealment and interference immunity of signal-code structures. It has been established that the modern electromagnetic environment is characterized by a high level of active, passive, and deceptive interference, as well as the widespread use of radio reconnaissance systems, which significantly complicates the provision of reliable and covert information transmission.

The influence of electronic countermeasures on the key parameters of communication channels, including the signal-to-noise ratio, synchronization, error probability, and channel capacity, has been analyzed. It is shown that under conditions of intensive interference, a complex degradation of radio channel characteristics occurs, thereby limiting the effectiveness of conventional information transmission methods.

The main approaches to improving concealment and interference immunity have been considered, including spread spectrum technologies, frequency hopping spread spectrum techniques, and the use of broadband signals. It has been established that existing methods have limitations in simultaneously ensuring a high level of concealment and resistance to modern radio reconnaissance systems.

The possibilities of applying timer signal structures as a promising basis for the formation of covert communication channels have been analyzed. Such structures provide an additional temporal degree of freedom in the process of information encoding.

Based on the conducted analysis, the expediency of further development of combined information transmission methods integrating timer signal structures and frequency hopping spread spectrum mechanisms has been substantiated. The purpose of

such integration is to increase the structural uncertainty and concealment of signals, as well as to reduce the probability of their detection, classification, and interception under conditions of electronic countermeasures.

The second chapter investigates the theoretical foundations of spread spectrum techniques and their role in ensuring information protection in radio communication systems. An analysis of direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) technologies is carried out, and their advantages and limitations in terms of interference immunity, energy concealment, and structural concealment of information transmission are identified.

Mathematical models of spread spectrum signals have been developed and analyzed, making it possible to formalize the processes of code and frequency energy dispersion, determine processing gain parameters, and assess the influence of spectrum bandwidth on energy concealment and resistance to intentional interference. The specific features of communication systems based on DSSS and FHSS are demonstrated, and the limitations of conventional methods associated with the presence of correlation features, synchronization dependence, and partial structural repetitiveness of signals are identified.

Combined spread spectrum techniques integrating code- and frequency-domain spreading mechanisms are investigated. It is shown that the combination of DSSS and FHSS provides an increase in processing gain, a reduction in power spectral density, improved communication channel survivability, and a lower probability of both energy-based and structural signal detection.

It has been established that the use of timer signal structures (TSS) provides an additional degree of structural uncertainty of signals through the utilization of temporal parameters for information encoding and an increase in the number of possible signal-code realizations. It is demonstrated that the integration of TSS with DSSS and FHSS techniques enables the generation of combined noise-like signals with enhanced concealment and resistance to detection.

he obtained results constitute the theoretical foundation for the further development of methods aimed at improving the concealment of information transmission based on the

integration of timer signal structures with frequency hopping spread spectrum techniques, which is considered in the subsequent chapter of the dissertation.

The third chapter investigates the theoretical foundations of timer signal structures as a basis for information protection by enhancing the structural concealment of signal-code structures in radio communication systems. The principles of constructing positional and non-positional signals are analyzed, and it is established that timer signal structures belong to the class of non-positional signals in which the information content is determined by the set of temporal intervals between significant modulation instants. It is shown that this approach provides an additional temporal degree of freedom for encoding and significantly expands the set of possible signal realizations.

Mathematical models of timer signal structures have been developed, and the regularities of their formation have been investigated. It has been established that the number of possible signal realizations is determined by the parameters of timer encoding and increases according to a combinatorial law, thereby providing a substantial enlargement of the signal ensemble compared to conventional positional codes.

An analysis of the spectral and correlation properties of timer signals has been carried out. It is shown that the irregular structure of temporal intervals forms a noise-like spectrum with reduced discrete components, which contributes to enhanced energy concealment and complicates the spectral detection of signals by radio reconnaissance systems. The autocorrelation and cross-correlation characteristics of timer signals have been investigated, and it has been established that their structure enables the formation of a wide ensemble of noise-like signal-code structures.

The specific features of correlation reception of timer signals have been studied. It is demonstrated that the use of conventional positional correlation receivers does not ensure correct reconstruction of timer signal structures due to the absence of fixed locations of information elements in the time domain, which results in the occurrence of local maxima in the correlation function and partial correlation matches.

It has been proven that the application of timer signal structures provides additional temporal uncertainty and increases the structural concealment of signals even prior to the application of traditional spread spectrum techniques. The obtained results establish the

theoretical basis for the further synthesis of combined information protection methods based on the integration of timer signals with direct sequence spread spectrum and frequency hopping spread spectrum technologies, which is considered in the subsequent chapter of the dissertation.

The fourth chapter of the dissertation develops and investigates methods for improving the concealment of information transmission based on the integration of timer signal structures with direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) technologies. An analysis of timer signal parameters is carried out, and it is established that their formation is based on inter-pulse intervals. It is shown that increasing these signal construction parameters leads to an exponential growth in the number of possible signal realizations and directly enhances the structural concealment of signals.

A comparative analysis of the spectral and energy efficiency of timer and positional signals is performed. It is established that timer signal structures are characterized by higher spectral efficiency due to the greater information density of their temporal structure, which confirms the feasibility of their application as a basis for the formation of noise-like signals in secure radio communication systems.

Methods for spreading the spectrum of timer signals based on DSSS and FHSS technologies are developed. For FHSS technology, algorithms for fast, slow, and multichannel frequency hopping adapted to the non-positional nature of timer signal structures are proposed. It is shown that the suggested approach ensures the integration of frequency-domain spread spectrum techniques without losing the properties of timer encoding and enables the formation of combined noise-like signals with an enhanced level of concealment.

The regularities governing the formation of structural concealment in combined signals are investigated, and it is established that structural concealment is determined by the combined effect of temporal, code, and frequency uncertainty. It is demonstrated that the contribution of FHSS depends not only on the number of available frequency positions but also on the number of frequency hops within a signal, which forms a set of possible frequency trajectories and further complicates signal reconstruction.

The performed analysis of the dependence of structural concealment on the parameters of timer signals, DSSS, and FHSS confirms its exponential growth with an increase in the combined signal basis. It is established that an increase in the integral signal basis is accompanied by enhanced entropy, noise-like properties, and interference immunity, thereby complicating signal detection, classification, and reconstruction by unauthorized monitoring systems. At the same time, it is shown that excessive spectrum spreading increases synchronization requirements and the complexity of communication system implementation, which substantiates the necessity of adaptively selecting the parameters of combined methods depending on the operating conditions of the communication system.

The conclusions of the dissertation summarize the results of the conducted research, formulate the main scientific findings and practical recommendations derived from the obtained results, and provide quantitative assessments of the effectiveness of the proposed methods and solutions under their application conditions.

The appendices contain materials concerning the implementation of the obtained results, as well as a list of the author's scientific publications and conference presentations related to the dissertation research.

Keywords: information protection, information transmission concealment, information and communication systems, radio communication systems, timer signal structures, frequency hopping spread spectrum, noise-like signals, spread spectrum, pseudorandom sequences, structural concealment, autocorrelation, cross-correlation, electronic countermeasures, interference immunity, signal-code structures, non-positional signals, information security.

ПЕРЕЛІК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Корчинський, В. В., Назаренко, О. А., Степанов, В. О., & Аль-Файюми, Х. (2022). Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів. *Інфокомунікаційні та комп'ютерні технології*, №2(02), 25–31. Київ: Відкритий міжнародний університет розвитку людини «Україна». – Режим доступу: <https://visn-icct.uu.edu.ua/index.php/icct/article/download/86/70>
2. Korchynskyi, V., Kildishev, V., Bektursunov, D., Havel, S., Stepanov, V., Slavych, V., & Petrovskyi, R. (2026). Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. *Technology Audit and Production Reserves*, №1(87), 18–24. – Режим доступу: <https://doi.org/10.15587/2706-5448.2026.353067> (Scopus)
3. Гавель, С., Корчинський, В., Степанов, В., & Куртіков, М. (2026). Методи підвищення криптографічної стійкості псевдовипадкових послідовностей на основі генераторів хаосу. *Herald of Khmelnytskyi National University. Technical Sciences*, 363(2), 149–154. – Режим доступу: <https://doi.org/10.31891/2307-5732-2026-363-19>
4. Korchynskyi, V., Havel, S., Sevastieiev, Ye., Petrovskyi, R., Slavych, V., Stepanov, V., & Riabukha, O. (2026). Methods of forming noise-like signals based on chaotic sequences and spline approximation. *Advances in Cyber-Physical Systems*, Vol. 11, No. 11, 50–55. Lviv Polytechnic National University. – Режим доступу: <https://doi.org/10.23939/acps2026.01.050>
5. Корчинський, В., Рябуха, О., Степанов, В., Голев, Д., & Лімарь, І. (2025). Пристрій захисту мовного акустичного сигналу в умовах радіоелектронної боротьби. *Measuring and Computing Devices in Technological Processes*, 82(2), 187–192. – Режим доступу: <https://doi.org/10.31891/2219-9365-2025-82-25>
6. Король, Я., Степанов, В., & Петренко, Ю. (2024). Рекомендації щодо забезпечення зв'язку в умовах застосування противником засобів радіоелектронної боротьби. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №5(5), 45–56. – Режим доступу:

<http://perspectives.pp.ua/index.php/niu/article/view/17627/17689>

7. Бібік, А. В., Городиський, Р. О., Ваврічен, О. А., & Степанов, В. О. (2026). Підвищення стійкості оперативного радіозв'язку в умовах сучасних загроз: потенціал мереж TETRA для підрозділів сектору безпеки та оборони й органів охорони державного кордону України. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №1(18), 69–83. – Режим доступу: [https://doi.org/10.52058/3041-1793-2026-1\(18\)-69-83](https://doi.org/10.52058/3041-1793-2026-1(18)-69-83)

Наукові праці, які засвідчують апробацію матеріалів дисертації:

8. 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. 17–18.

9. Степанов В.О., Петренко Ю.А., Корчинський В.В., Назаренко О.А. Підвищення завадозахищеності систем зв'язку на основі розширення спектра таймерних сигналів. Науково-технічна конференція 'Системи і технології зв'язку, інформатизації та кібербезпеки: Військовий інститут телекомунікацій та інформатизації імені Герої Крут, 1 грудня 2022 року Київ. 2022. 202-203. – Режим доступу: <https://mitit.mil.gov.ua/api/files/2173>

10. Корчинський В.В. Підвищення прихованості передавання шумоподібних сигнально-кодкових конструкцій на основі таймерних сигналів / В.В. Корчинський, В.О. Степанов // Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. К.: НУОУ, 2023. 84-87. – Режим доступу: <https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view>

11. Корчинський В.В. Методи захисту інформації на основі розширення спектра сигналу / В.В. Корчинський, О. М. Рябуха, Ю. В. Белова, Степанов В.О. // VII International Scientific and Practical Conference «Scientific Paradigm in the Context of Technologies and Society Development» held on July 16-18, 2024 in Geneva, Switzerland, 216-220. – Режим доступу:

<https://archive.interconf.center/index.php/conference-proceeding/issue/view/16-18.07.2024>

12. Bielova Iuliia, Stepanov Vadym, Bohdaniuk Ihor, Manankov Roman. Intelligent ai-based siem systems for detection and analysis of cyber incidents // Development of science in the XXI century. Proceedings of the V International Scientific and Practical Conference. Marseille. France. 2025. 159-160. DOI <https://doi.org/10.5281/zenodo.18115841>

13. Корчинський В.В., Кільдішев В.Й., Степанов В.О., Богданюк І.А., Ярема В.В., Поліщук О.В., Бельська І. С. Комбінований метод захисту інформації на основі криптографічних алгоритмів, завадостійких кодів та методів розширення спектра. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. 317-321. – Режим доступу: <https://suitt.edu.ua/wp-content/uploads/2026/03/zbirnyk-tez-duitz-80-mntk.pdf>

14. Дослідження застосування радіостанцій “Німера” G1 Pro та ретранслятора В1 у бойовій системі “Кропива”, з метою покращення спроможностей автоматизованих систем тактичної ланки управління/ Юрій ПЕТРЕНКО, Ігор ШЕВЕЛЬОВ, Вадим СТЕПАНОВ// Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану// Військова академія (м. Одеса)/ Збірник тез доповідей VII Міжнародної науково-практичної конференції 17 жовтня 2025 року. Секція 11. Актуальні проблеми безпеки та оборони в умовах сучасних воєнних конфліктів – с. 515-516. – Режим доступу: <https://vaodesa.mil.gov.ua/wp-content/uploads/2025/12/zbirnyk.pdf>

15. 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. С. 543. – Режим доступу: <https://impeer.org.ua/wp-content/uploads/2025/07/%D0%9C%D0%9E%D0%9D%D0%9E%D0%93%D0%A0%D0%90%D0%A4%D0%86%D0%AF-26-06-2024.pdf>

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	22
ВСТУП	23
РОЗДІЛ 1. АНАЛІЗ ТА ОГЛЯД МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ШИРОКОСМУГОВИХ СИГНАЛІВ	30
1.1 Огляд сучасних вітчизняних засобів завадозахищених систем радіозв'язку.....	30
1.2 Аналіз показників прихованості передавання інформації в системах радіозв'язку.....	34
1.3 Вплив енергетичної та спектральної ефективності каналу на енергетичну прихованість систем радіозв'язку	40
1.4 Засоби радіорозвідки та методи виявлення сигналів	43
1.5 Методи забезпечення прихованості передавання інформації в системах радіозв'язку	47
1.6 Недоліки класичних методів розширення спектра та проблема забезпечення структурної прихованості сигналів.....	52
1.7 Постановка задачі дослідження та обґрунтування переходу до таймерних сигнальних конструкцій	56
1.8 Висновки до розділу 1	58
РОЗДІЛ 2. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА ТА ПСЕВДОВИПАДКОВОГО ПЕРЕСКОКУ РОБОЧОЇ ЧАСТОТИ.....	60
2.1 Класифікація методів розширення спектра та їх роль у захисті інформації.....	60
2.2 Математичні моделі сигналів з розширеним спектром.....	62
2.3 Метод прямого розширення спектра для захисту інформації.....	64
2.4 Методи псевдовипадкового перескоку робочої частоти	67
2.5 Комбіновані методи розширення спектра	71
2.6 Обґрунтування використання таймерних сигналів для підвищення прихованості передавання інформації.....	76

2.7 Висновки до розділу 2	80
РОЗДІЛ 3. ТАЙМЕРНІ СИГНАЛЬНІ КОНСТРУКЦІЇ ТА ЇХ ВЛАСТИВОСТІ У СИСТЕМАХ ПРИХОВАНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ СТАТИСТИЧНОГО ШИФРУВАННЯ	
3.1 Дослідження статистичних і кореляційних властивостей таймерних сигнальних конструкцій для захисту інформації	83
3.2 Вплив кореляційних властивостей таймерних сигналів на формування шумоподібних сигналів	95
3.3 Аналіз кореляційного приймання позиційних та непозиційних шумоподібних сигналів.....	97
3.4 Алгоритм кореляційного приймання шумоподібних таймерних сигнальних конструкцій на основі аналізу екстремумів інтегральної функції	104
3.5 Оцінка ефективності методів захисту інформації на основі ширококутових сигналів	106
3.6 Висновки до розділу 3	111
РОЗДІЛ 4. РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕТОДІВ РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ	
4.1 Аналіз параметрів таймерних сигнальних конструкцій для реалізації маніпуляції та розширення спектра	113
4.2 Порівняльний аналіз спектральної та енергетичної ефективності позиційних і таймерних сигналів.....	118
4.3 Розробка методів розширення спектра таймерних сигналів на основі псевдовипадкового перескоку робочих частот	122
4.3.1 Аналіз методів ППРЧ для позиційних сигналів.....	122
4.3.2 Метод швидкого ППРЧ для розширення спектра таймерних сигналів.....	125
4.3.3 Метод повільного ППРЧ для розширення спектра таймерних сигналів.....	127
4.3.4 Метод багатоканального ППРЧ для таймерних сигналів.....	129
4.4 Розробка комбінованого методу розширення спектра таймерних сигналів....	132

4.5 Оцінювання структурної прихованості та інтегральної бази комбінованого сигналу.....	137
4.6 Ентропійний аналіз та адаптивне керування параметрами шумоподібного таймерного сигналу	144
4.7 Висновки до розділу 4	147
ВИСНОВКИ	152
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	154
ДОДАТОК А. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА	167
ДОДАТОК Б. АКТИ ВПРОВАДЖЕННЯ	170
ДОДАТОК В. ІНТЕРФЕЙС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТАЙМЕРНИХ СИГНАЛІВ.....	172

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

РЕП – радіоелектронна протидія

ППРЧ – псевдовипадкове перескоку робочої частоти

АКФ – автокореляційна функція

ВКФ – взаємкореляційна функція

ІКС – інформаційно-комунікаційна система

НСД – несанкціонований доступ

СКК – сигнально-кодова конструкція

ЗММ – значущий момент модуляції;

ЗМВ – значущий момент відтворення;

ЧМ – частотна модуляція;

ФМ – фазова модуляція;

ПВП – псевдовипадкова послідовність

ПРС-ПВП – пряме розширення спектра псевдовипадковими послідовностями

РЕБ – радіоелектронна боротьба

РЕР – радіоелектронна розвідка

С/Ш – відношення сигнал/шум

ТСК – таймерна сигнальна конструкція

ШСС – широкосмуговий сигнал

FHSS (Frequency Hopping Spread Spectrum) – технологія розширення спектра методом псевдовипадкового перескоку частоти

DSSS (Direct Sequence Spread Spectrum) – технологія прямого розширення спектра

BER (Bit Error Rate) – ймовірність бітової помилки

SNR (Signal-to-Noise Ratio) – відношення сигнал/шум

ВСТУП

Актуальність. Розвиток систем радіозв'язку супроводжується зростанням вимог до захисту передавання інформації в умовах активного застосування засобів радіоелектронної боротьби та радіоелектронної розвідки. Поширення високочутливих систем моніторингу спектра, засобів цифрової обробки сигналів і методів інтелектуального аналізу електромагнітного середовища суттєво підвищує ймовірність виявлення, класифікації та перехоплення сигналів зв'язку. За таких умов забезпечення прихованості передавання інформації стає одним із ключових напрямів розвитку перспективних інформаційно-комунікаційних систем.

Захист інформації на фізичному рівні передавання, зокрема із застосуванням класичних методів модуляції та окремих технологій розширення спектра, забезпечує певний рівень завадозахищеності, проте не завжди дозволяє одночасно досягти високих показників енергетичної, структурної та часової прихованості. Зокрема, використання прямого розширення спектра або псевдовипадкового перескоку робочих частот окремо характеризується наявністю структурних або часових закономірностей, які можуть бути використані сучасними засобами радіорозвідки для виявлення та часткової реконструкції параметрів сигналу.

У цьому контексті особливого значення набуває застосування непозиційних сигнально-кодових конструкцій, серед яких перспективне місце займають таймерні сигнальні конструкції. На відміну від класичних позиційних сигналів, таймерні сигнали реалізують процес передавання інформації шляхом зміни часових інтервалів між значущими моментами модуляції, що формує додатковий часовий ступінь свободи та забезпечує підвищення структурної невизначеності сигналів. Непозиційний характер таймерних сигналів дозволяє значно розширити ансамбль можливих сигнальних реалізацій, зменшити вираженість регулярних спектральних складових та ускладнити процеси їх кореляційного і спектрального аналізу.

Суттєвий внесок у розвиток теорії захисту інформації на основі методів розширення спектра зробили вітчизняні та зарубіжні науковці, зокрема Е. Фауре, Л.

Політанський, Р. Політанський В. Гордійчук, М. Захарченко, В. Кільдішев, А. Семенко, Б. Радзімовський, А. Камінський та інші. Разом із тим питання інтеграції таймерних сигнальних конструкцій із методами псевдовипадкового перескоку робочих частот, а також дослідження властивостей сформованих комбінованих шумоподібних сигналів залишаються недостатньо опрацьованими.

Перспективним напрямом підвищення прихованості є поєднання часового, частотного та кодового розширення спектра шляхом інтеграції таймерних сигнальних конструкцій із технологіями псевдовипадкового перескоку робочих частот. Такий підхід дозволяє формувати широкосмугові шумоподібні сигнали зі складною багаторівневою структурою, для яких процеси виявлення, класифікації та відновлення параметрів суттєво ускладнюються. При цьому структурна прихованість визначається не лише кількістю доступних частот або кодових послідовностей, але й множиною можливих часових і частотних траєкторій формування сигналу.

У зв'язку з цим актуальним науковим завданням є розроблення моделей, методів і алгоритмів підвищення прихованості передавання інформації в системах радіозв'язку на основі інтеграції таймерних сигнальних конструкцій із псевдовипадковим перескоком робочих частот, що забезпечують формування комбінованих шумоподібних сигналів із підвищеною структурною невизначеністю та зниженням їх детектованості в умовах радіоелектронного протиборства.

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

Дисертаційна робота виконана відповідно до основних положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах» та Стратегії кібербезпеки України. Тема дослідження пов'язана з науковими напрямами, визначеними в п. 1.2.9 «Теорія та комп'ютерні технології інформаційної безпеки» та п. 1.2.9.5 «Кібербезпека інформаційно-комунікаційних систем» документа «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і

гуманітарних наук Національної академії наук України на 2024–2028 роки», затвердженого постановою Президії НАН України від 10.01.2024 № 8.

Тематика дисертаційного дослідження відповідає стандарту вищої освіти та фаховим компетентностям освітньо-наукової програми підготовки докторів філософії за спеціальністю 125 «Кібербезпека» Державного університету інтелектуальних технологій і зв'язку Міністерства освіти і науки України та спрямована на проведення фундаментальних і прикладних досліджень у галузі захисту інформації, зокрема на розроблення методів підвищення прихованості передавання даних із використанням таймерних сигнальних конструкцій, широкосмугових шумоподібних сигналів і псевдовипадкових послідовностей.

Дисертаційна робота виконувалася в межах держбюджетної науково-дослідної роботи «Розроблення методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах на основі інтегрованих сигнально-кодових перетворень» (державний реєстраційний номер 0126U002946). Основні результати дисертаційного дослідження увійшли до складу науково-технічного звіту за зазначеною науково-дослідною роботою.

Метою дисертаційної роботи є розроблення методів захисту інформації в інформаційно-комунікаційних системах шляхом підвищення прихованості передавання на основі інтеграції таймерних сигнальних конструкцій із методами псевдовипадкового перескоку робочих частот для формування комбінованих шумоподібних сигналів із підвищеною структурною невизначеністю та стійкістю до виявлення, аналізу і несанкціонованого перехоплення.

Для досягнення поставленої мети необхідно було вирішити наступні науково-технічні задачі:

- 1) провести аналіз загроз безпеці інформації в інформаційно-комунікаційних системах, що функціонують в умовах радіоелектронної протидії, та дослідити вплив засобів радіоелектронної розвідки і навмисних завад на прихованість передавання інформації;

- 2) дослідити існуючі методи розширення спектра сигналів, зокрема пряме розширення спектра та псевдовипадковий перескок робочих частот, визначити їх

переваги, обмеження та можливості щодо забезпечення захисту інформації від виявлення, перехоплення та аналізу засобами технічної розвідки, а також оцінити їх вплив на енергетичну, структурну і часову прихованість передавання інформації в інформаційно-комунікаційних системах;

3) дослідити закономірності формування таймерних сигнальних конструкцій з урахуванням їх спектральних, кореляційних характеристик та кодової відстані, а також оцінити вплив параметрів побудови сигнально-кодових конструкцій на рівень структурної прихованості, стійкість до структурного аналізу та захищеність передавання інформації в інформаційно-комунікаційних системах;

4) розробити метод інтеграції таймерних сигнальних конструкцій із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот для формування комбінованих шумоподібних сигнально-кодових конструкцій, які характеризуються підвищеним рівнем структурної невизначеності та забезпечують підвищення захищеності інформаційного обміну в інформаційно-комунікаційних системах;

5) розробити математичний апарат оцінювання структурної прихованості комбінованих сигнально-кодових конструкцій та встановити закономірності впливу параметрів їх формування на рівень структурної невизначеності сигналів, що є кількісною характеристикою захищеності інформаційного обміну від засобів радіоелектронної розвідки та несанкціонованого перехоплення;

6) провести дослідження ефективності запропонованих методів та оцінити вплив параметрів комбінованих шумоподібних сигналів на показники структурної прихованості та захищеності передавання інформації від виявлення, аналізу і перехоплення в умовах радіоелектронної протидії.

Об'єкт дослідження – процеси прихованого передавання інформації в системах радіозв'язку в умовах радіоелектронної протидії.

Предмет дослідження – методи формування та інтеграції таймерних сигнальних конструкцій і псевдовипадкового перескоку робочих частот для підвищення прихованості передавання інформації в системах радіозв'язку.

Методи дослідження. У дисертаційній роботі використано методи теорії інформації, теорії зв'язку, теорії сигналів і систем, теорії кодування, теорії ймовірностей та теорії прихованості передавання інформації. Положення теорії прихованості використано для дослідження показників енергетичної, структурної та часової прихованості сигналів, а також для оцінювання рівня захищеності передаваної інформації від несанкціонованого доступу, виявлення, класифікації та перехоплення засобами радіоелектронної розвідки. Методи системного аналізу застосовано для дослідження особливостей функціонування систем радіозв'язку в умовах радіоелектронної протидії та визначення вимог до забезпечення прихованості передавання інформації. Методи математичного аналізу та комбінаторики використано для розроблення математичних моделей таймерних сигнальних конструкцій, дослідження закономірностей їх формування та оцінювання кількості можливих сигнально-кодових реалізацій. Методи спектрального, кореляційного та статистичного аналізу застосовано для дослідження властивостей таймерних сигналів, оцінювання їх шумоподібності, енергетичної та структурної прихованості. Методи математичного та імітаційного моделювання використано для розроблення комбінованих методів формування шумоподібних сигналів на основі інтеграції таймерних сигнальних конструкцій із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот, а також для дослідження впливу параметрів сигналів на показники прихованості та завадозахищеності. Методи чисельного експерименту та порівняльного аналізу застосовано для оцінювання ефективності запропонованих методів, визначення залежностей структурної прихованості від параметрів таймерного кодування, прямого розширення спектра та псевдовипадкового перескоку робочих частот, а також для порівняння отриманих результатів із відомими методами захисту інформації.

Наукова новизна одержаних результатів полягає в наступному:

1. *Вперше* розроблено метод підвищення захищеності інформаційного обміну в інформаційно-комунікаційних системах на основі інтеграції таймерних сигнальних конструкцій, прямого розширення спектра та псевдовипадкового

перескоку робочих частот, який, на відміну від існуючих методів, забезпечує формування комбінованих шумоподібних сигнально-кодових конструкцій з підвищеним рівнем часової, кодової та частотної невизначеності, що ускладнює виявлення, структурний аналіз і несанкціоноване перехоплення інформації.

2. *Вперше* одержано аналітичні залежності структурної прихованості від параметрів таймерних сигнальних конструкцій, псевдовипадкових послідовностей та алгоритмів псевдовипадкового перескоку робочих частот, які дають змогу прогнозувати рівень захищеності передавання інформації від засобів радіоелектронної розвідки та несанкціонованого перехоплення шляхом оцінювання структурної невизначеності сформованих сигнально-кодових конструкцій і встановлюють експоненційний характер зростання кількості можливих сигнальних реалізацій залежно від параметрів їх формування.

3. *Набув подальшого розвитку* математичний апарат оцінювання структурної прихованості комбінованих шумоподібних сигнально-кодових конструкцій, який враховує сукупний внесок таймерного кодування, прямого розширення спектра та псевдовипадкового перескоку робочих частот і, на відміну від існуючих методів, дає змогу визначати інтегральний рівень структурної невизначеності сигналів з урахуванням часових, кодових та частотних параметрів їх формування, що дозволяє оцінювати ефективність методів захисту інформації на фізичному рівні та рівень захищеності інформаційного обміну в умовах радіоелектронної протидії.

4. *Вперше* встановлено залежність між кодовою відстанню та коефіцієнтами взаємної кореляції таймерних сигнальних конструкцій, що дозволило обґрунтувати умови формування слабокорельованих ансамблів сигналів із заданими властивостями структурної прихованості та завадозахищеності, які сприяють підвищенню рівня захищеності інформаційного обміну в умовах радіоелектронної протидії.

5. *Удосконалено* метод формування шумоподібних сигнально-кодових конструкцій на основі таймерних сигналів шляхом їх інтеграції з технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот, який, на відміну від існуючих методів для позиційних кодів, забезпечує реалізацію

швидкої, повільної та багатоканальної перебудови частоти без втрати властивостей непозиційного таймерного кодування та дозволяє підвищити рівень захищеності інформаційного обміну в умовах радіоелектронної протидії за рахунок збільшення структурної невизначеності сформованих сигналів.

Практична значимість отриманих результатів полягає у тому, що розроблені методи, математичні моделі та алгоритми можуть бути використані під час проєктування, модернізації та оцінювання захищеності інформаційно-комунікаційних систем, які функціонують в умовах радіоелектронної протидії, з метою підвищення рівня захисту інформації від виявлення, перехоплення та несанкціонованого доступу.

1. Запропонований метод інтеграції таймерних сигнальних конструкцій із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот забезпечує формування комбінованих шумоподібних сигналів із підвищеним рівнем структурної прихованості та сприяє підвищенню захищеності інформаційного обміну в інформаційно-комунікаційних системах в умовах радіоелектронної протидії.

2. Розроблений математичний апарат та одержані аналітичні залежності структурної прихованості можуть бути використані під час створення засобів захисту інформації в інформаційно-комунікаційних системах для кількісного оцінювання рівня захищеності інформаційного обміну від засобів радіоелектронної розвідки та несанкціонованого перехоплення. Практичне застосування запропонованого методу показало, що при зміні параметрів таймерних сигнальних конструкцій у межах $m = 4 \dots 10$, $s = 2 \dots 8$, кількості інформаційних відрізків $i = 2 \dots 6$, використанні псевдовипадкових послідовностей із рівнем структурної прихованості $S_{\text{ПВП}} = 16 \dots 128$ двійкових вимірів та алгоритмів псевдовипадкового перескоку робочих частот із рівнем структурної прихованості $S_{\text{ППРЧ}} = 32 \dots 480$ двійкових вимірів досягнуто інтегральний рівень структурної прихованості комбінованих сигналів від 53 до 631 двійкового виміру, що відповідає множині можливих сигнальних реалізацій порядку $2^{53} - 2^{631}$.

3. Одержані результати можуть бути використані під час проєктування та модернізації систем захищеного радіозв'язку для обґрунтованого вибору параметрів таймерного кодування, прямого розширення спектра та псевдовипадкового перескоку робочих частот відповідно до заданих вимог безпеки. Практичне застосування отриманих залежностей дозволило встановити, що збільшення параметрів таймерного кодування, прямого розширення спектра та псевдовипадкового перескоку робочих частот приводить до квазілінійного зростання структурної прихованості та експоненційного збільшення кількості можливих сигнальних реалізацій, що забезпечує підвищення стійкості інформаційного обміну до виявлення, аналізу та перехоплення.

4. Встановлена залежність між кодовою відстанню та коефіцієнтами взаємної кореляції таймерних сигнальних конструкцій може бути використана під час формування ансамблів шумоподібних сигналів із заданими показниками прихованості та завадостійкості. Отримані результати дозволяють обґрунтовано здійснювати відбір слабкорельованих сигнальних конструкцій для зменшення рівня міжсигнальних завад і підвищення ефективності кореляційного приймання. Практичне застосування запропонованого методу показало, що зі збільшенням кодової відстані від 1Δ до 7Δ коефіцієнти взаємної кореляції зменшуються від 0,882–0,870 до 0,149–0,078, а для окремих пар сигналів наближаються до нуля. Це підтверджує можливість формування слабкорельованих ансамблів таймерних сигнальних конструкцій з мінімальною кодовою відстанню $d_{\text{мшт}}(\Delta) > 1$, що забезпечує одночасне підвищення структурної прихованості, завадостійкості та ефективності передавання інформації в умовах радіоелектронної протидії.

5. Удосконалений метод формування шумоподібних сигналів дозволяє реалізувати швидку, повільну та багатоканальну перебудову робочої частоти для таймерних сигнальних конструкцій без втрати властивостей непозиційного кодування. Результати досліджень показали, що сформовані ансамблі ТСК характеризуються середнім коефіцієнтом взаємної кореляції $\bar{r} \approx 0,64$ та коефіцієнтом ортогональності $K_{\text{орт}} \approx 0,36$, що підтверджує можливість їх практичного використання для побудови шумоподібних сигналів із підвищеною

структурною прихованістю та завадозахищеністю в системах радіозв'язку спеціального призначення.

5. Результати дисертаційної роботи можуть бути використані в інформаційно-комунікаційних системах спеціального призначення, системах військового та відомчого радіозв'язку, під час розроблення перспективних засобів захисту інформації, а також у навчальному процесі закладів вищої освіти під час викладання дисциплін, пов'язаних із теорією сигналів, захистом інформації та системами спеціального зв'язку.

Отримані в роботі результати впроваджені в навчальний процес кафедри Кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, що підтверджується відповідним актом впровадження. Практична цінність роботи в тому, що отримані результати придатні для інженерного проектування радіотехнічних та телекомунікаційних систем, що підтверджено актом впровадження основних результатів досліджень на підприємстві ТОВ «БФ «Секрет Сервіс».

Особистий внесок здобувача. Основні наукові та практичні результати дослідження отримані автором особисто. В дисертаційній роботі використані лише ті з результатів, що були опубліковані у наукових працях у співавторстві, які є індивідуальним внеском автора.

Основні положення та результати дисертаційної роботи отримані автором самостійно. Автор виконав усі теоретичні та практичні дослідження, що становить основу дисертаційної роботи. При цьому в роботах, що написані в співавторстві, здобувачу належить: [1] – розробка алгоритму розширення спектра таймерних сигнальних конструкцій на основі псевдовипадкового перескоку робочої частоти; [2] – аналіз якісних та кількісних показників при вирішенні завдання прямого розширення спектра таймерних сигнальних конструкцій; [3] – розробка алгоритму побудови псевдовипадкових послідовностей на основі генераторів хаосу; [4] – аналіз отриманих результатів щодо алгоритму формування шумоподібних сигналів на основі хаотичних послідовностей та сплайнової апроксимації; [5] – проведення експериментальної частини роботи, аналіз та обговорення результатів

дослідження; [6] – аналіз сучасних засобів радіоелектронної боротьби, дослідження впливу радіоелектронного подавлення на функціонування систем радіозв'язку, розробленні рекомендацій щодо підвищення стійкості та прихованості передавання інформації в умовах радіоелектронної протидії; [7] – дослідження можливостей підвищення захищеності та стійкості оперативного радіозв'язку в умовах радіоелектронної протидії, аналіз переваг використання технології TETRA для забезпечення безпечного інформаційного обміну, узагальненні результатів дослідження та формулюванні висновків щодо практичного застосування мереж TETRA в системах зв'язку сектору безпеки та оборони.

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження доповідалися, обговорювалися та отримали схвалення на міжнародних і всеукраїнських науково-практичних конференціях, семінарах та вебінарах, зокрема: V Міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси, 2017); Науково-технічній конференції «Системи і технології зв'язку, інформатизації та кібербезпеки» (Київ, 2022); IV науково-практичному вебінарі «Забезпечення кібероборони держави» (Київ, 2023); VII International Scientific and Practical Conference «Scientific Paradigm in the Context of Technologies and Society Development» (Geneva, Switzerland, 2024); 80-й ювілейній Міжнародній науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів і студентів Державного університету інтелектуальних технологій і зв'язку (Одеса, 2025); VII Міжнародній науково-практичній конференції «Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану» (Одеса, 2025).

Результати досліджень апробовано під час обговорення питань підвищення прихованості передавання інформації в системах радіозв'язку, застосування таймерних сигнальних конструкцій, методів розширення спектра сигналів та псевдовипадкового перескоку робочих частот в умовах радіоелектронної протидії.

Публікації. За результатами досліджень по темі дисертаційної роботи опубліковано 15 наукових праць, у тому числі: 7 наукових статей у періодичних виданнях України [1-7], що включені до переліку наукових фахових видань України,

в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів, у тому числі одна стаття [2] у журналі, який цитується у наукометричній базі даних Scopus; 8 тез доповідей [7-15] в матеріалах наукових конференцій. Крім зазначених, участь у 1 ініціативної НДР за спеціальною тематикою.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, трьох додатків, списку використаних джерел і містить 121 сторінок основного тексту, 13 рисунків, 7 таблиць, 7 сторінок додатків. Список використаних джерел містить 98 найменувань і займає 13 сторінок. Загальний обсяг роботи складає 173 сторінки.

У роботі використовувався інструмент штучного інтелекту (ШІ) ChatGPT для пошуку літератури та граматичної перевірки тексту. Всі розділи, при написанні яких використовувався ШІ, перевірені та відредаговані автором особисто. Наукові положення, висновки та результати є власним інтелектуальним внеском автора.

РОЗДІЛ 1

АНАЛІЗ ТА ОГЛЯД МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ШИРОКОСМУГОВИХ СИГНАЛІВ

У розділі надано аналіз умов функціонування систем радіозв'язку в умовах радіоелектронної протидії, а також розглянуто основні методи захисту інформації від несанкціонованого доступу шляхом підвищення прихованості та завадостійкості передавання сигнально-кодових конструкцій. Встановлено, що сучасне радіоелектронне середовище характеризується високим рівнем активних, пасивних та імітаційних завад, а також широким застосуванням засобів радіорозвідки, що суттєво ускладнює забезпечення стійкого та прихованого передавання інформації. Визначено обмеження класичних методів щодо забезпечення структурної прихованості та обґрунтовано перспективність використання непозиційних таймерних сигнальних конструкцій як засобу формування додаткової часової невизначеності. На основі проведеного аналізу визначено напрями подальших досліджень, пов'язаних із розробленням комбінованих методів захисту інформації на основі інтеграції таймерних сигнальних конструкцій і псевдовипадкового перескоку робочої частоти.

1.1 Огляд сучасних вітчизняних засобів завадозахищених систем радіозв'язку

Функціонування систем радіозв'язку в сучасних умовах воєнних конфліктів характеризується суттєвим ускладненням радіоелектронної обстановки [1, 2], що зумовлено активним застосуванням засобів радіоелектронної протидії (РЕП). РЕП є складовою радіоелектронної боротьби та охоплює комплекс організаційних і технічних заходів, спрямованих на порушення роботи систем радіозв'язку противника, а також на захист власних радіоелектронних засобів. До основних складових РЕП відносять радіоелектронну розвідку, радіоелектронне подавлення

та радіоелектронний захист, які функціонують у взаємозв'язку та формують єдину систему впливу на радіоканали [3, 4].

Аналіз ведення бойових дій в Україні свідчить про необхідність заміни застарілих радіостанцій виробництва «Motorola» [5] на сучасні захищені системи зв'язку, оскільки існуючі радіостанції не мають функцій псевдовипадкового переналаштування робочої частоти (ППРЧ), не підтримують роботу у самоорганізуючій мережі MESH/MANET, а швидкість передавання даних не відповідає вимогам автоматизованих систем управління [6]. Ситуація погіршилася з розвитком застосування БпЛА, стрими яких працюють лише через широкосмугові високошвидкісні канали зв'язку, наразі для цих цілей використовуються супутникова мережа «Starlink» та мережі національних операторів. Окремою проблемою стало використання ключів шифрування типу AES-256 [7], адже для радіостанцій «Motorola» потрібно придбавати платні ключі виробництва США. У 2024 році Начальником Головного управління зв'язку та кібербезпеки Генерального штабу Збройних Сил України були погоджені «Особливості тактичних радіостанцій «Himera» G1 Pro», основна увага приділялася вбудованим технологіям стрибкоподібної зміни частоти (FHSS) з метою боротьби з засобами радіоелектронної розвідки та радіоелектронного придушення. На відміну від «Motorola», національні комплекти «Himera» G1 Pro здатні самостійно генерувати ключі AES-256 без необхідності зовнішнього вводу, що усуває залежність від іноземних виробників, що особливо актуально в умовах війни, коли доступ до зовнішніх ресурсів може бути обмежений [9]. Дослідні зразки обладнання були розроблені та передані на випробування до Сил оборони України, а Збройні сили США придбали українські станції для використання на військових аеродромах, що свідчить про їхню ефективність та конкурентоздатність на міжнародному рівні. На кафедрі Загальновійськових дисциплін Військової академії (м. Одеса) проводилося макетування та тестування 8 комплектів «Himera» G1 Pro і двох ретрансляторів «Himera» B1. За результатами тестування підтверджена повна сумісність обладнання «Himera» з бойовими системами Збройних Сил України. Макетування здійснювалося на п'яти автоматизованих робочих місцях (АРМ) у складі робочого

планшету з завантаженою бойовою системою «Кропива» версії V6.17.0 та радіостанцією «Himera» G1 Pro. Для збільшення дальності роботи застосовувалися ретранслятори В1. За результатами макетування були відпрацьовані завдання щодо створення зон розвідки, постановки задач на ведення розвідки в визначених зонах особовому складу спостережних пунктів, а також опрацювання питань виявлення та нанесення в геоінформаційну систему десятків цілей з визначенням координат. Підтверджено повну сумісність «Himera» G1 Pro з програмним забезпеченням «Кропива». В подальшому планується перевірка уніфікації програмного забезпечення БПЛА та бойової системи «Кропива» за допомогою утиліти «Борти». За результатами макетування та тестування підтверджені наступні технічні характеристики «Himera» G1 Pro: стандарт шифрування AES-256 з самостійним генеруванням ключів, псевдовипадкове переналаштування робочої частоти (ППРЧ) до 100 стрибків/сек за технологією FHSS, спеціалізований Android-додаток, підтримка MESH/MANET мереж, вбудований GPS з обміном геолокацією в реальному часі, голосова комунікація, обмін текстовими повідомленнями та даними зі швидкістю 38,4 кбіт/с, низька ймовірність виявлення та перехоплення завдяки протидії РЕБ та РЕР. Радіостанція важить 270 г, має потужність передавача 0,2–1 Вт, чутливість радіоприймача -100 дБм, діапазон робочих частот 310–670 МГц, бездротовий інтерфейс Bluetooth LE 5.0, роз'єм антени SMA-J та роз'єм зарядки/гарнітури/даних M12 8-pin.

Порівняно з «Motorola» DP-4800, «Himera» G1 Pro має переваги за більшістю параметрів [5,6]: самостійне генерування ключів AES-256 усуває залежність від зовнішніх виробників, наявність ППРЧ (FHSS) до 100 стрибків/сек підвищує завадозахищеність, підтримка MESH/MANET мереж забезпечує гнучкість мережі, вбудований GPS дозволяє обмін геолокацією, швидкість передачі даних 38,4 кбіт/с відповідає вимогам автоматизованих систем, а вартість 15 000 грн значно нижча за 32–37 000 грн для «Motorola». Водночас, «Motorola» має перевагу за потужністю передавача (1–5 Вт проти 0,2–1 Вт у «Himera»), що може забезпечувати більшу дальність зв'язку на місцевості зі складним рельєфом. Однак низька потужність «Himera» компенсується високою завадозахищеністю завдяки технології FHSS та

широкому діапазону частот (310–670 МГц), що дозволяє ефективно працювати в умовах активних завад.

Система «Кропива» на базі радіостанцій «Himera» G1 Pro та ретрансляторів В1 пропонує комплексне рішення для підвищення стійкості радіозв'язку в умовах радіоелектронної протидії (РЕП). Її переваги порівняно з DMR, який аналізувався раніше, включають високу прихованість завдяки шифруванню AES-256 та технології FHSS, що унеможливорює виявлення структури мережі засобами РЕП, наприклад, комплексами «Торн-М». Низька ймовірність виявлення та перехоплення досягається завдяки стрибкоподібній зміні частоти до 100 стрибків/сек, а широкий діапазон частот (310–670 МГц) забезпечує гнучкість у виборі каналів та уникнення завад. Технологія FHSS дозволяє підтримувати зв'язок при низькому співвідношенні сигнал/шум, ускладнюючи роботу засобів РЕБ, таких як Р-330Ж «Житель». Підтримка MESH/MANET мереж дозволяє формувати самоорганізуючі мережі, які автоматично відновлюють зв'язок при знищенні окремих вузлів, а обмін геолокацією та інтеграція з бойовою системою «Кропива» забезпечують автоматизацію процесу управління. Економічна ефективність досягається завдяки нижчій вартості та незалежності від зовнішніх виробників.

Незважаючи на переваги, система «Кропива» має деякі обмеження, які вимагають подальших досліджень [5, 6]. По-перше, потужність передавача 0,2–1 Вт може бути недостатньою для роботи на великих відстанях у складному рельєфі, однак для вирішення цієї проблеми застосовуються ретранслятори В1, які здатні працювати автономно до 14 діб. По-друге, необхідно дослідження уніфікації програмного забезпечення БпЛА-розвідників з бойовою системою «Кропива» за допомогою утиліти «Борти». По-третє, потрібно експериментально перевірити дальність зв'язку при використанні ретранслятора В1 для оптимізації розгортання мережі. По-четверте, необхідно дослідження масштабованості системи для великих підрозділів, наприклад, батальйонного рівня.

Отже, дослідження застосування радіостанцій «Himera» G1 Pro та ретранслятора В1 у бойовій системі «Кропива» підтверджує, що ця система є ефективним вітчизняним рішенням для підвищення стійкості радіозв'язку в умовах

РЕБ [9-11]. Її переваги включають високу прихованість завдяки шифруванню AES-256 [11] та технології FHSS, завадозахищеність завдяки стрибкоподібній зміні частоти та широкому діапазону, адаптивність завдяки підтримці MESH/MANET мереж та автоматизації управління [6], а також економічну ефективність завдяки нижчій вартості та незалежності від зовнішніх виробників. Водночас, для повномасштабного впровадження в ДПСУ та ЗСУ необхідно продовжити дослідження сумісності з БпЛА та іншими системами зв'язку, оптимізувати розгортання мережі з використанням ретрансляторів В1 для збільшення дальності зв'язку, а також порівняти ефективність з міжнародними стандартами, такими як TETRA, за критеріями прихованості, завадозахищеності та масштабованості [9, 10].

Отже, особливості функціонування систем радіозв'язку в умовах радіоелектронної протидії визначаються складною взаємодією між параметрами каналу, характеристиками завад та можливостями засобів радіоелектронної розвідки. Це обумовлює необхідність використання широкосмугових, шумоподібних та таймерних сигнальних конструкцій із розширеним спектром і псевдовипадковою перебудовою параметрів як перспективного напрямку підвищення прихованості та стійкості військового радіозв'язку. Модель функціонування систем радіозв'язку в умовах радіоелектронної протидії надана на рис. 1.1.

1.2 Аналіз показників прихованості передавання інформації в системах радіозв'язку

Захист передаваної інформації в системах радіозв'язку в умовах сучасної радіоелектронної протидії значною мірою визначається рівнем прихованості функціонування радіосистем [12,13]. Засоби радіоелектронної розвідки противника орієнтовані не лише на виявлення факту радіообміну, але й на визначення параметрів сигналу, розкриття його структури та подальше встановлення змісту повідомлень або організацію ефективного радіоелектронного подавлення [14].

У зв'язку з цим прихованість передавання інформації слід розглядати як комплексну властивість системи зв'язку, що характеризує її здатність протистояти процесам виявлення, перехоплення, класифікації та інформаційного аналізу сигналів.

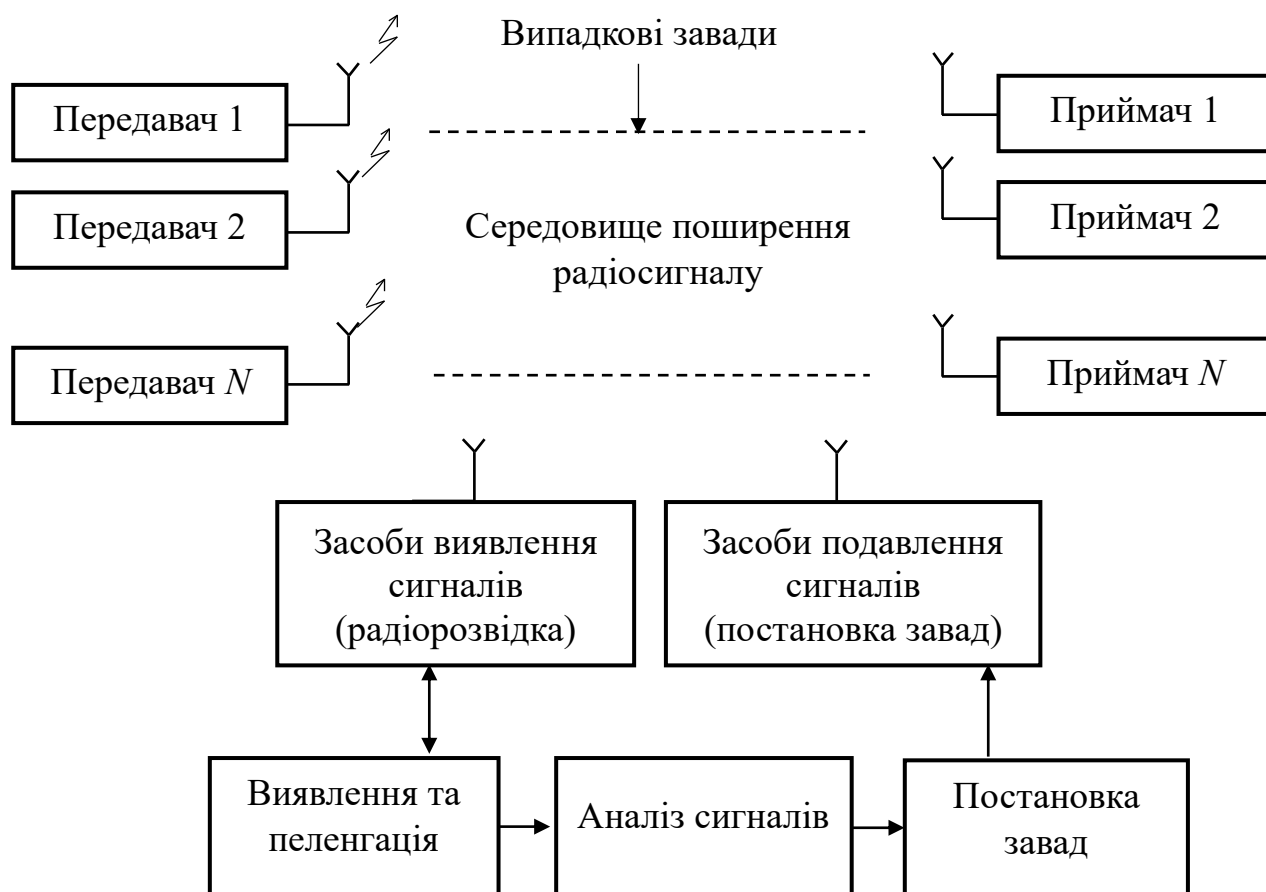


Рис. 1.1. Модель функціонування систем радіозв'язку в умовах радіоелектронної протидії

У теорії захищеного радіозв'язку прихованість поділяють на енергетичну, структурну та інформаційну [13]. Кожна з цих складових відповідає певному етапу роботи засобів радіоелектронної розвідки та характеризує окремий аспект захисту передавання інформації.

Першою складовою є енергетична прихованість [13], яка характеризує здатність системи протидіяти виявленню самого факту існування сигналу в каналі зв'язку. Засоби радіорозвідки зазвичай застосовують енергетичні детектори, що

приймають рішення про наявність сигналу шляхом порівняння енергії прийнятого процесу із заданим порогом. Для такого випадку задача виявлення описується двома гіпотезами:

$$\begin{cases} H_0: x(t) = n(t), \\ H_1: x(t) = s(t) + n(t), \end{cases} \quad (1.1)$$

де $n(t)$ – шум або завадовий процес, $s(t)$ – корисний сигнал.

Статистика енергетичного детектора визначається як [10, 11]

$$Y = \int_0^T |x(t)|^2 dt, \quad (1.2)$$

де T – інтервал спостереження.

Рішення про наявність сигналу приймається шляхом порівняння статистики Y з пороговим значенням γ :

$$Y \underset{H_0}{\overset{H_1}{\geq}} \gamma. \quad (1.3)$$

Основними показниками роботи детектора є ймовірність правильного виявлення сигналу $P_{\text{вияв}}$ та ймовірність помилкової тривоги $P_{\text{пт}}$. Оскільки прихованість є характеристикою, оберненою до виявлення, кількісну оцінку енергетичної прихованості доцільно визначати як

$$P_{\text{сн}} = 1 - P_{\text{вияв}}. \quad (1.4)$$

Таким чином, чим меншою є ймовірність виявлення сигналу засобами радіорозвідки, тим вищою є енергетична прихованість системи. Ключовим параметром, що визначає можливість виявлення, є відношення сигнал/шум

$$\frac{S}{N} = \frac{P_s}{P_n}, \quad (1.5)$$

де P_s – потужність сигналу, P_n – потужність шуму або завади.

У системах із розширеним спектром, зокрема при реалізації псевдовипадкового перескоку робочої частоти (ППРЧ), досягнення енергетичної прихованості забезпечується шляхом зниження спектральної густини потужності сигналу. Загальне визначення спектральної густини [15,16] потужності має вигляд

$$S(f) = \lim_{T \rightarrow \infty} \frac{|X_T(f)|^2}{T}, \quad (1.6)$$

де $X_T(f)$ – спектр сигналу на інтервалі спостереження T .

Для систем ППРЧ середня спектральна густина потужності може бути оцінена співвідношенням [20]

$$S_{\text{ППРЧ}}(f) \approx \frac{P_s}{B_{FH}}, \quad (1.7)$$

де B_{FH} – смуга перебудови частоти. Збільшення смуги перестроювання призводить до зменшення спектральної густини потужності та ускладнює енергетичне виявлення сигналу засобами радіорозвідки.

Після виявлення сигналу наступним етапом роботи засобів радіоелектронної розвідки є його перехоплення та визначення структури. Цей етап характеризується структурною прихованістю, яка визначає ступінь невизначеності щодо параметрів сигнальної конструкції, типу модуляції, часової структури та принципів формування сигналу.

Кількісно структурну прихованість доцільно розглядати як ентропійну міру невизначеності вибору сигнальної конструкції [13]:

$$S_{\text{стр}} = \log_2 L_{\text{СКК}}, \quad (1.8)$$

де $L_{СКК}$ – кількість можливих сигнально-кодкових конструкцій або варіантів організації фізичного каналу. Зростання ансамблю сигнальних конструкцій призводить до підвищення невизначеності для станції розвідки та ускладнює процес структурного аналізу.

Важливим проміжним етапом є також перехоплення сигналу, тобто отримання достатнього обсягу радіовипромінювання для подальшого аналізу. Цей показник характеризується ймовірністю $P_{пер}$, яка залежить від часу роботи передавача, режимів випромінювання, параметрів сканування та швидкості перебудови частоти.

Кількісною характеристикою структурної прихованості може бути ймовірність розкриття структури сигналу $P_{стр}$, яка визначається за умови, що сигнал уже виявлений та перехоплений [12,13].

Третім рівнем є інформаційна прихованість, що характеризує здатність системи захищати смисловий зміст повідомлення після виявлення та аналізу структури сигналу [13]. На цьому етапі противник намагається розкрити інформацію шляхом криптоаналізу, статистичного аналізу або перебору ключів.

Для симетричних криптографічних систем простір ключів визначається як [11]

$$N_k = 2^{L_k}, \quad (1.9)$$

де L_k – довжина криптографічного ключа. За умови атаки повним перебором ймовірність випадкового вгадування ключа оцінюється як

$$P_{бр} = 2^{-L_k}. \quad (1.10)$$

Однак у загальному випадку інформаційна прихованість визначається не лише довжиною ключа, а також часовими та ресурсними обмеженнями противника:

$$P_{\text{інф}} = f(L_k, T_{\text{переб}}, R_{\text{обч}}), \quad (1.11)$$

де $T_{\text{переб}}$ – час перебору ключового простору, $R_{\text{обч}}$ – доступні обчислювальні ресурси. Отже, інформаційна прихованість є комплексною характеристикою криптографічної стійкості системи.

Оскільки процес радіоелектронної розвідки складається з послідовних етапів – виявлення, перехоплення, структурного аналізу та інформаційного розкриття – загальний рівень успішності розвідки може бути оцінений як добуток відповідних імовірностей. За припущення статистичної незалежності цих етапів отримаємо

$$P_{\text{розв}} = P_{\text{вияв}} \cdot P_{\text{пер}} \cdot P_{\text{стр}} \cdot P_{\text{інф}}. \quad (1.12)$$

Якщо завдання розвідки обмежується лише визначенням параметрів системи для організації радіоелектронного подавлення, тоді інформаційне розкриття не є необхідним і $P_{\text{інф}} = 1$. У такому випадку

$$P_{\text{розв}} = P_{\text{вияв}} \cdot P_{\text{пер}} \cdot P_{\text{стр}}. \quad (1.13)$$

Якщо ж для організації радіопротидії достатньо лише встановлення факту передавання сигналу, тоді

$$P_{\text{розв}} = P_{\text{вияв}}. \quad (1.14)$$

Аналіз наведених показників свідчить, що різні методи захисту по-різному впливають на складові прихованості. Класичні криптографічні алгоритми забезпечують переважно інформаційну прихованість, однак практично не впливають на можливість виявлення сигналу. Методи розширення спектра, зокрема ППРЧ, ефективно підвищують енергетичну прихованість, знижуючи спектральну густину потужності сигналу та ускладнюючи його перехоплення. Водночас

класичні системи ППРЧ не повністю усувають можливість структурного аналізу, оскільки закономірності перебудови частоти та часові параметри сигналу можуть бути частково ідентифіковані сучасними засобами радіоелектронної розвідки.

У зв'язку з цим перспективним напрямом розвитку захищених систем радіозв'язку є застосування таймерних сигнальних конструкцій, які поряд із частотною невизначеністю формують також часову невизначеність сигналу. Поєднання технології псевдовипадкового перескоку робочої частоти з таймерними сигнальними конструкціями створює передумови для одночасного підвищення енергетичної, структурної та інформаційної прихованості передавання, що обумовлює необхідність подальшого дослідження таких методів у наступних розділах дисертаційної роботи.

1.3 Вплив енергетичної та спектральної ефективності каналу на енергетичну прихованість систем радіозв'язку

Енергетична прихованість систем радіозв'язку значною мірою визначається параметрами каналу передавання інформації, серед яких особливе місце займають енергетична та спектральна ефективність [12,13]. Дані характеристики відображають взаємозв'язок між енергетичними витратами на передавання інформації, шириною використовуваної смуги частот та можливістю виявлення сигналу засобами радіоелектронної розвідки. Оскільки станції радіорозвідки приймають рішення про наявність сигналу на основі аналізу його енергетичних характеристик та спектральної густини потужності, вибір параметрів каналу безпосередньо впливає на рівень енергетичної прихованості системи.

Енергетична ефективність характеризує мінімальні енергетичні витрати, необхідні для передавання одного біта інформації із заданою якістю приймання, та визначається співвідношенням [15,16]

$$\beta = \frac{E_b}{N_0}, \quad (1.15)$$

де E_b – енергія, що припадає на один інформаційний біт, N_0 – спектральна густина потужності шуму. Чим менше значення E_b/N_0 , при якому забезпечується задана ймовірність помилки, тим вищою є енергетична ефективність системи.

Спектральна ефективність визначає ступінь використання смуги частот і характеризується відношенням швидкості передавання інформації до ширини займаного спектра [18]:

$$\gamma = \frac{R_b}{B}, \quad (1.16)$$

де R_b – швидкість передавання інформації, B – ширина смуги сигналу. Показник γ характеризує кількість інформації, переданої в одиниці спектрального ресурсу, і вимірюється в біт/с/Гц.

Між енергетичною та спектральною ефективністю існує фундаментальний взаємозв'язок, що випливає з теореми Шеннона для каналу з адитивним білим гаусівським шумом [19]:

$$C = B \log_2 \left(1 + \frac{S}{N} \right), \quad (1.17)$$

де C – пропускна здатність каналу. Поділивши (1.16) на ширину смуги B та врахувавши співвідношення

$$\frac{S}{N} = \gamma \frac{E_b}{N_0}, \quad (1.18)$$

одержимо граничну залежність між енергетичною та спектральною ефективністю [19]:

$$\frac{E_b}{N_0} = \frac{2^\gamma - 1}{\gamma}. \quad (1.19)$$

Залежність (1.19) є фундаментальною межею Шеннона і демонструє компроміс між енергетичними витратами та ефективністю використання спектра. Зі збільшенням спектральної ефективності унеобхідне значення E_b/N_0 зростає нелінійно, що вимагає підвищення енергетичних витрат або застосування складніших методів кодування й оброблення сигналів.

Енергетична прихованість безпосередньо пов'язана з потужністю випромінювання передавача та спектральною густиною потужності сигналу. Для каналу радіозв'язку потужність сигналу на вході приймача визначається рівнянням передачі Фріса [20]:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R} \right)^2, \quad (1.20)$$

де P_t – потужність передавача, G_t і G_r – коефіцієнти підсилення антен, λ – довжина хвилі, R – дальність. З рівняння (1.20) випливає, що дальність виявлення сигналу засобами радіоелектронної розвідки зростає зі збільшенням потужності випромінювання:

$$R_{\text{вияв}} \propto \sqrt{P_t}. \quad (1.21)$$

Тому зменшення потужності передавача або зниження спектральної густини потужності безпосередньо підвищує енергетичну прихованість. Спектральна густина потужності сигналу визначається як [20]

$$S(f) \approx \frac{P_t}{B}. \quad (1.22)$$

З виразу (1.22) можна побачити, що при незмінній потужності розширення спектра сигналу призводить до зменшення його спектральної густини потужності, а отже – до зниження ймовірності енергетичного виявлення.

У вузькосмугових системах із високою спектральною ефективністю енергія сигналу концентрується у відносно малій смузі частот, що формує підвищену спектральну густину потужності та спрощує роботу енергетичних детекторів. Натомість у системах із розширеним спектром, зокрема ПРС-ПВП та ППРЧ, енергія сигналу розподіляється по значно ширшому частотному діапазону, внаслідок чого рівень спектральної густини потужності наближається до рівня шуму.

Для систем із псевдовипадковим перескоком робочої частоти середня спектральна густина потужності оцінюється виразом (1.7). Збільшення B_{FH} дозволяє підвищити енергетичну прихованість системи за рахунок зниження помітності сигналу для засобів радіорозвідки. Разом з тим класичні системи ППРЧ формують переважно частотну невизначеність і не повністю усувають можливість структурного аналізу часових параметрів сигналу.

Отже, енергетична та спектральна ефективність каналу формують взаємопов'язаний компроміс між якістю зв'язку, використанням спектрального ресурсу та рівнем енергетичної прихованості. Підвищення спектральної ефективності забезпечує більшу пропускну здатність, однак може супроводжуватися зростанням помітності сигналу. Натомість розширення спектра та зниження спектральної густини потужності підвищують енергетичну прихованість, що пояснює доцільність застосування технологій ППРЧ і створює передумови для подальшого дослідження таймерних сигнальних конструкцій у поєднанні з частотною перебудовою.

1.4 Засоби радіорозвідки та методи виявлення сигналів

Засоби радіорозвідки призначені для виявлення, перехоплення та аналізу радіовипромінювань у складній електромагнітній обстановці. Основними класами методів виявлення сигналів є енергетичне та структурне виявлення, а також методи просторової локалізації та спектрально-часового аналізу. Енергетичне виявлення базується на перевірці гіпотези про наявність сигналу за критерієм енергетичного

перевищення над рівнем шуму. Модель прийнятого сигналу може бути подана у вигляді $x(t) = s(t) + n(t)$, де $s(t)$ – корисний сигнал, $n(t)$ – адитивний шум.

Для виявлення наявності сигналу в ефірі на рис. 1.2 наведена структура енергетичного детектора.

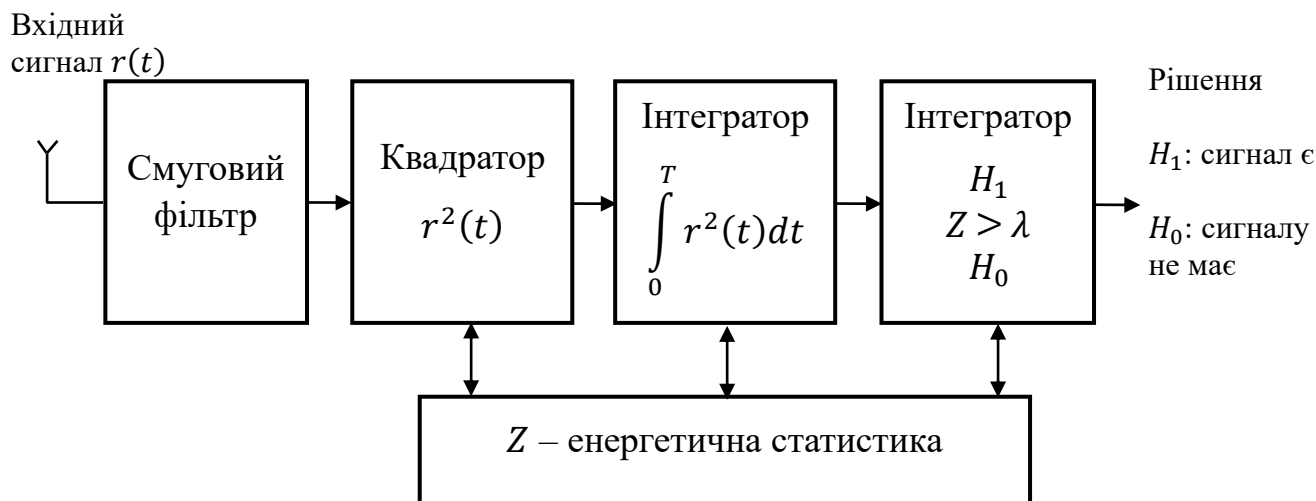


Рис. 1.2. Структура енергетичного детектора

Енергетичний детектор є одним із основних засобів радіорозвідки для енергетичного виявлення сигналів на тлі шуму. Його робота ґрунтується на перевірці гіпотези про наявність сигналу за критерієм енергетичного перевищення над рівнем шуму. Структура детектора включає послідовно з'єднані блоки: смуговий фільтр, квадратор, інтегратор. Смуговий фільтр виділяє смугу частот, у якій очікується наявність сигналу, та пригнічує завади поза цією смугою. Квадратор здійснює множення вхідного сигналу $r(t)$ на себе, перетворюючи його в $r^2(t)$, що дозволяє виділити енергетичну компоненту сигналу. Інтегратор на інтервалі часу T обчислює енергетичну статистику за формулою [19,20]:

$$E = \int_0^T |x(t)|^2 dt. \quad (1.23)$$

Рішення про наявність сигналу приймається за правилом:

$$E \geq_{H_0}^{H_1} \lambda, \quad (1.24)$$

де H_0 – гіпотеза відсутності сигналу, H_1 – наявність сигналу, λ – порогове значення. Для випадку адитивного білого гаусівського шуму ймовірність хибної тривоги визначається як:

$$P_{FA} = \Pr(E > \lambda | H_0). \quad (1.25)$$

Структурне виявлення базується на кореляційній обробці сигналів. Кореляційний приймач використовує статистику [22]:

$$R_{xs} = \int_0^T x(t)s(t) dt, \quad (1.26)$$

де максимальне значення кореляції вказує на наявність сигналу з відомою структурою. Для цифрових реалізацій часто використовується дискретна кореляція:

$$R[k] = \sum_{n=0}^{N-1} x[n] s[n-k]. \quad (1.27)$$

Пеленгування сигналів здійснюється на основі вимірювання різниці фаз або часу приходу сигналу на просторово рознесені антени. Для фазового методу різниця фаз визначається як:

$$\Delta\varphi = \frac{2\pi d \sin(\theta)}{\lambda}, \quad (1.28)$$

де d – відстань між антенами, λ – довжина хвилі, θ – кут приходу сигналу.

Оцінка напрямку приходу сигналу може бути подана як [15,16]:

$$\theta = \arcsin\left(\frac{\Delta\varphi\lambda}{2\pi d}\right). \quad (1.29)$$

Аналіз спектральних характеристик сигналів виконується через перетворення Фур'є [16]:

$$S(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt, \quad (1.30)$$

що дозволяє визначати зайнятість спектра, структуру модуляції та ознаки шумоподібності сигналу. Часовий аналіз сигналів базується на оцінці автокореляційної функції [16]:

$$R_{xx}(\tau) = \int_{-\infty}^{\infty} x(t)x(t + \tau)dt, \quad (1.31)$$

яка використовується для виявлення періодичності та структурних закономірностей у сигналі.

На рис. 1.3 представлені залежності щільності ймовірності енергетичної статистики [19], які ілюструють принцип роботи енергетичного детектора при виявленні сигналів на тлі шуму.

Ліва крива відображає розподіл щільності ймовірності $p_z(z | H_0)$ для гіпотези H_0 , яка відповідає ситуації, коли в каналі присутній лише шум без корисного сигналу. Цей розподіл зазвичай має експоненціальний або хі-квадратний характер і характеризується тим, що його максимум розташований біля нуля, оскільки енергія чистого шуму зазвичай низька.

Права крива ілюструє розподіл $p_z(z | H_1)$ для гіпотези H_1 , коли в каналі присутній сигнал разом із шумом. Ця крива зсунута вправо відносно попередньої, оскільки наявність сигналу збільшує значення енергетичної статистики, а її форма залежить від потужності сигналу та характеристик шуму.

Вертикальна пунктирна лінія на обох графіках позначає порогове значення λ , яке використовується для прийняття рішення про наявність сигналу: якщо значення енергетичної статистики перевищує цей поріг, приймається гіпотеза H_1 про

наявність сигналу, інакше – гіпотеза H_0 про його відсутність. При цьому ймовірність хибної тривоги визначається площею під лівою кривою праворуч від порогу λ , а ймовірність пропуску сигналу – площею під правою кривою ліворуч від цього порогу.

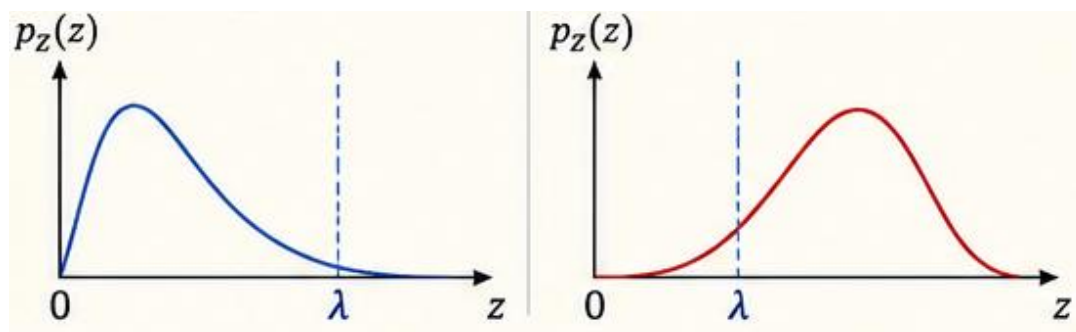


Рис. 1.3. Залежності щільності ймовірності енергетичної статистики, які ілюструють принцип роботи енергетичного детектора

Оптимальний вибір порогу λ дозволяє мінімізувати сумарну ймовірність помилок, а чим далі розподіли для гіпотез H_0 та H_1 віддалені один від одного, тим вища достовірність виявлення сигналу енергетичним детектором.

Отже, сучасні засоби радіорозвідки поєднують енергетичні, кореляційні, спектральні та просторові методи аналізу, що дозволяє ефективно виявляти навіть слабкі та шумоподібні сигнали в умовах радіоелектронної протидії.

1.5 Методи забезпечення прихованості передавання інформації в системах радіозв'язку

У сучасних умовах ведення бойових дій ефективність систем військового радіозв'язку значною мірою визначається їх здатністю забезпечувати приховане та завадостійке передавання інформації в умовах активної радіоелектронної протидії. Засоби радіоелектронної розвідки та подавлення здатні здійснювати виявлення, перехоплення, класифікацію та придушення радіосигналів, що потребує застосування комплексних методів захисту. До основних напрямків забезпечення

прихованості та завадозахищеності відносять криптографічний захист, методи розширення спектра, псевдовипадковий перескок робочої частоти, а також використання широкосмугових і шумоподібних сигналів.

Одним із базових механізмів захисту інформації є криптографічне перетворення даних. Його основне призначення полягає у забезпеченні конфіденційності та цілісності повідомлень навіть у випадку перехоплення сигналу противником. У системах військового зв'язку найбільш поширеним є симетричне шифрування, зокрема алгоритми сімейства AES. Загальна модель криптографічного захисту може бути подана у вигляді [11]

$$C = E_K(M), \quad (1.32)$$

де M – повідомлення, K – ключ шифрування, $E_K(\cdot)$ – функція криптографічного перетворення, C – зашифрований текст. На приймальній стороні здійснюється розшифрування [11]

$$M = D_K(C), \quad (1.33)$$

де $D_K(\cdot)$ – функція розшифрування.

Однак криптографічний захист забезпечує лише прихованість змісту повідомлення, але не приховує сам факт радіообміну. Радіоелектронна розвідка здатна виявляти джерело випромінювання за енергетичними та часово-частотними характеристиками сигналу. Тому поряд із шифруванням використовуються фізичні методи приховання передачі.

Одним із найефективніших напрямків є застосування технологій розширення спектра, які дозволяють збільшувати ширину спектра сигналу значно більше мінімально необхідної для передавання інформації. Основною перевагою такого методу є зниження спектральної густини потужності сигналу та підвищення його стійкості до навмисних завад. Коефіцієнт розширення спектра визначається як [16]

$$G_p = \frac{B_s}{B_i}, \quad (1.34)$$

де B_s – ширина спектра розширеного сигналу, B_i – інформаційна смуга.

У децибельній формі процесинговий виграш становить [16]

$$G_{p(dB)} = 10 \log_{10} \left(\frac{B_s}{B_i} \right). \quad (1.35)$$

Чим більший коефіцієнт розширення, тим складніше виявити сигнал і тим вищою є його завадостійкість.

Одним із найбільш поширених методів розширення спектра є DSSS (Direct Sequence Spread Spectrum) – пряме розширення спектра псевдовипадковою послідовністю (ПРС-ПВП). У цьому випадку інформаційна послідовність множиться на високошвидкісний псевдовипадковий код [18]:

$$s(t) = m(t)c(t), \quad (1.36)$$

де $m(t)$ – інформаційний сигнал, $c(t)$ – псевдовипадкова послідовність, $s(t)$ – сформований широкосмуговий сигнал.

Унаслідок такого множення спектр сигналу суттєво розширюється, а його енергетична густина зменшується. На приймальній стороні використовується кореляційна обробка із синхронізованою копією коду [18]:

$$R(\tau) = \int s(t)c(t - \tau) dt. \quad (1.37)$$

Максимум кореляційної функції відповідає правильній синхронізації та дозволяє виділити корисний сигнал на фоні шуму і завад.

Іншим поширеним методом є ППРЧ – розширення спектра шляхом псевдовипадкового перескоку робочої частоти. Суть методу полягає у швидкій

перебудові несучої частоти відповідно до закону, визначеного псевдовипадковою послідовністю [21,22]:

$$f_n = f_0 + \Delta f \cdot k_n, \quad (1.38)$$

де f_0 – початкова частота, Δf – крок перебудови, k_n – елемент псевдовипадкової послідовності. Передавач і приймач синхронно змінюють частоту роботи, що ускладнює процес радіорозвідки та постановки ефективних завад. Імовірність ураження каналу вузькосмуговою завадою можна оцінити як [24,25]

$$P_j = \frac{B_j}{B_h}, \quad (1.39)$$

де B_j – смуга завади, B_h – сумарний діапазон перебудови частот.

Зі збільшенням діапазону ППРЧ ймовірність успішного подавлення сигналу зменшується [24,25]. ППРЧ забезпечує не лише завадостійкість, але й певний рівень енергетичної та структурної прихованості, оскільки противнику необхідно одночасно визначити частотний план, алгоритм перебудови та синхронізацію. Проте класичні системи ППРЧ мають обмеження, пов'язані з можливістю статистичного аналізу частотних переходів та прогнозування закону перебудови за недостатньої криптографічної стійкості керуючих послідовностей.

Важливим напрямком розвитку військових систем зв'язку є застосування широкосмугових та шумоподібних сигналів. Шумоподібний сигнал характеризується властивостями, близькими до випадкового процесу, та має низьку взаємну кореляцію з іншими сигналами. Його енергетичний спектр може бути описаний спектральною густиною потужності [26]

$$S(f) = \lim_{T \rightarrow \infty} \frac{|x_T(f)|^2}{T}, \quad (1.40)$$

де $X_T(f)$ – спектр сигналу за інтервал спостереження T . Для оцінювання енергетичної прихованості використовується відношення сигнал/шум

$$SNR = \frac{P_s}{P_n}, \quad (1.41)$$

де P_s – потужність сигналу, P_n – потужність шуму. При зменшенні спектральної густини потужності широкосмуговий сигнал може перебувати нижче порогу виявлення засобів радіорозвідки [26].

Водночас класичні методи ПРС-ПВП та ППРЧ мають низку обмежень. Метод ПРС-ПВП потребує високоточної синхронізації та може бути виявлений за наявності відомих структурних ознак псевдовипадкових кодів. Класичний ППРЧ забезпечує частотну маскувальну властивість [26], однак не приховує часову структуру передавання та може бути підданий стистичному аналізу. Крім того, обидва методи вразливі до широкосмугових загороджувальних завад і сучасних автоматизованих систем РЕР [27].

Для оцінювання пропускної здатності каналу в умовах завад використовується формула Шеннона (1,17). Зниження SNR під впливом РЕП безпосередньо призводить до зменшення пропускної здатності та достовірності передавання інформації.

Таким чином, сучасні системи військового радіозв'язку потребують комплексного застосування криптографічних механізмів, технологій розширення спектра та методів псевдовипадкової перебудови частоти. Разом із тим обмеження класичних ПРС-ПВП і ППРЧ свідчать про необхідність подальшого розвитку методів структурної та часової прихованості, зокрема шляхом використання широкосмугових таймерних сигнальних конструкцій і ППРЧ, що становить основу подальших досліджень у дисертаційній роботі.

1.6 Недоліки класичних методів розширення спектра та проблема забезпечення структурної прихованості сигналів

Розширення спектра є одним із найбільш ефективних напрямів забезпечення завадозахищеності та прихованості передавання інформації в системах радіозв'язку [12-14]. До найбільш поширених технологій такого типу відносять системи з ПРС-ПВП і ППРЧ. Застосування цих методів дозволяє підвищити стійкість до активних завад, зменшити спектральну густину потужності сигналу та ускладнити його виявлення засобами радіоелектронної розвідки [28-30]. Однак розвиток сучасних засобів радіоелектронної боротьби та цифрової обробки сигналів [31,32] виявив низку обмежень класичних технологій розширення спектра, що потребує їх подальшого вдосконалення.

У системах ПРС-ПВП розширення спектра досягається шляхом множення інформаційної послідовності на високошвидкісний псевдовипадковий код. У результаті спектр сигналу розширюється, а його енергетична щільність зменшується. Обробний виграш системи ПРС-ПВП визначається як [34,35]

$$G_p = \frac{B_{\text{ПВП}}}{B_d}, \quad (1.42)$$

де $B_{\text{ПВП}}$ – ширина спектра після розширення, B_d – ширина спектра інформаційного сигналу. Збільшення G_p забезпечує підвищення завадостійкості та зменшення спектральної густини потужності сигналу [36]

$$S(f) \approx \frac{P_t}{B_{\text{ПВП}}}, \quad (1.43)$$

де P_t – потужність передавача. Незважаючи на очевидні переваги метод ПРС-ПВП має суттєві обмеження. Насамперед це необхідність синхронізації псевдовипадкових послідовностей у передавачі та приймачі. Втрата синхронізації призводить до різкого погіршення якості приймання та збільшення ймовірності

помилки. Крім того, сучасні засоби радіорозвідки здатні використовувати кореляційні методи пошуку, які дозволяють виявляти сигнали з ПРС-ПВП навіть при низьких рівнях спектральної густини потужності.

У системах ППРЧ розширення спектра реалізується шляхом псевдовипадкової перебудови несучої частоти відповідно до закону частотних стрибків. Середня ширина використовуваного спектра визначається як [34,35]

$$B_{\text{ППРЧ}} = N_f \Delta f, \quad (1.44)$$

де N_f – кількість частотних позицій, Δf – крок перебудови. Обробний виграш систем ППРЧ може бути оцінений виразом [26,37]

$$G_{\text{ППРЧ}} = \frac{B_{\text{ППРЧ}}}{B_s}, \quad (1.45)$$

де B_s – смуга окремого частотного каналу.

Розширення спектра за рахунок частотних стрибків забезпечує зниження ймовірності прицільного подавлення та ускладнює роботу вузькосмугових завад. Середня спектральна густина потужності при цьому визначається як [26]

$$S_{\text{ППРЧ}}(f) \approx \frac{P_t}{B_{\text{ППРЧ}}}. \quad (1.46)$$

Однак класичні системи ППРЧ також мають низку недоліків. Основною проблемою є те, що ППРЧ забезпечує переважно частотну невизначеність, залишаючи часову структуру сигналу відносно регулярною. Тривалість перебування на частоті, періодичність стрибків і параметри синхронізації часто залишаються детермінованими або квазидетермінованими, що створює передумови для структурного аналізу.

Сучасні комплекси радіорозвідки використовують багатоканальні приймачі, цифровий спектральний моніторинг та алгоритми машинної обробки сигналів,

здатні накопичувати інформацію про частотні стрибки та реконструювати закон перебудови частоти. Ймовірність виявлення сигналу при енергетичному контролі визначається залежністю [33-35]

$$P_d = f\left(\frac{E_b}{N_0}, P_{fa}, T_{obs}\right), \quad (1.47)$$

де P_{fa} – ймовірність помилкової тривоги, T_{obs} – час спостереження. Зі збільшенням часу спостереження T_{obs} навіть сигнали з низькою спектральною густиною потужності можуть бути виявлені шляхом накопичення енергії.

Після енергетичного виявлення сигналу виникає наступний етап роботи засобів радіорозвідки – структурне виявлення, тобто встановлення внутрішньої організації сигналу, параметрів модуляції, алгоритму перебудови частоти та синхронізаційних характеристик. Імовірність успішного структурного аналізу може бути подана як [33]

$$P_{str} = f(T_{obs}, N_h, Q_s), \quad (1.48)$$

де N_h – кількість зафіксованих частотних переходів, Q_s – сукупність структурних ознак сигналу.

Для класичних систем ППРЧ збільшення кількості спостережуваних переходів N_h призводить до зростання ймовірності визначення закону перебудови робочих частот та параметрів синхронізації [35]. Таким чином, хоча сигнал може залишатися енергетично малопомітним, його структура з часом стає доступною для аналізу.

Особливої актуальності проблема структурного виявлення набуває в умовах використання автоматизованих комплексів РЕР, які поєднують енергетичне виявлення, спектральний аналіз та статистичне накопичення даних. У таких системах регулярність часової структури ППРЧ стає демаскувальною ознакою, яка

може бути використана для організації ефективного радіоподавлення або перехоплення.

Порівняльний аналіз методів розширення спектра, наведений у табл. 1.1, дозволяє оцінити їх можливості щодо забезпечення прихованості та завадозахищеності передавання інформації в системах радіозв'язку. Найбільш поширеними технологіями розширення спектра є методи ПРС-ПВП та ППРЧ, кожен із яких характеризується власними перевагами та обмеженнями.

Таблиця 1.1

Переваги та обмеження методів розширення спектра

Метод	Переваги	Обмеження
ПРС-ПВП	Високий обробний виграш, зниження спектральної густини потужності, стійкість до вузькосмугових завад	Складна синхронізація, можливість кореляційного виявлення
ППРЧ	Стійкість до прицільних завад та РЕБ, ефективне використання частотної невизначеності	Регулярність часової структури та можливість накопичення частотних переходів
ТСК та ППРЧ	Формування частотної та часової невизначеності, підвищена структурна прихованість	Підвищена алгоритмічна та апаратна складність

Метод ПРС-ПВП забезпечує розширення спектра шляхом множення інформаційної послідовності на псевдовипадковий код, що дозволяє зменшити спектральну густину потужності сигналу та отримати значний обробний виграш. Це підвищує стійкість до вузькосмугових завад і частково ускладнює енергетичне виявлення сигналу засобами радіоелектронної розвідки. Разом із тим основними обмеженнями ПРС-ПВП залишаються високі вимоги до кореляційної синхронізації та можливість виявлення сигналу за допомогою кореляційних методів обробки, особливо у випадку накопичення статистики спостереження.

Метод ППРЧ реалізує розширення спектра за рахунок псевдовипадкової зміни робочої частоти відповідно до заданого алгоритму перебудови. Такий підхід забезпечує високу стійкість до вузькосмугових і прицільних завад, а також

ускладнює процес радіоподавлення, оскільки противнику необхідно відстежувати закон перебудови частоти. Проте класичні системи ППРЧ формують переважно частотну невизначеність, тоді як часова структура сигналу та параметри частотних переходів часто залишаються регулярними. Це створює передумови для реконструкції алгоритму ППРЧ і подальшого структурного аналізу сигналу сучасними засобами радіоелектронної розвідки.

Перспективним напрямом розвитку методів розширення спектра є інтеграція ППРЧ із непозиційними ТСК [36-40]. Поєднання ТСК та ППРЧ [38,39] дозволить одночасно формувати частотну та часову невизначеність сигналу, що суттєво ускладнить не лише його енергетичне виявлення, а й структурний аналіз. На відміну від класичних систем ППРЧ [27, 28], де послідовність частотних переходів може бути накопичена та проаналізована, використання таймерного кодування змінює часову структуру сигналу та ускладнює визначення закономірностей його формування. Водночас даний підхід характеризується підвищеною алгоритмічною та апаратною складністю, що пов'язано з необхідністю забезпечення точного формування часових параметрів і синхронізації.

Отже, наведене порівняння свідчить, що класичні методи ПРС-ПВП та ППРЧ забезпечують переважно енергетичну прихованість, однак не повністю усувають проблему структурного виявлення сигналів. Це обґрунтовує доцільність дослідження комбінованих методів, заснованих на інтеграції ППРЧ із таймерними сигнальними конструкціями, які здатні забезпечити більш високий рівень загальної прихованості передавання інформації.

1.7 Постановка задачі дослідження та обґрунтування переходу до таймерних сигнальних конструкцій

Проведений аналіз показників прихованості передавання інформації, впливу енергетичної та спектральної ефективності каналу, а також сучасних методів розширення спектра свідчить про те, що забезпечення захисту інформації в системах радіозв'язку в умовах радіоелектронної протидії є складною

багатокритеріальною задачею. Сучасні системи радіозв'язку повинні одночасно забезпечувати високу енергетичну прихованість, тобто мінімальну ймовірність виявлення, стійкість до структурного аналізу та здатність функціонувати в умовах активного радіоелектронного подавлення. Аналіз існуючих методів розширення спектра показав, що найбільш поширені технології ПРС-ПВП та ППРЧ забезпечують суттєве підвищення енергетичної прихованості та стійкості до завад. Разом із тим проведений аналіз дозволяє зробити висновок, що класичні методи розширення спектра не забезпечують повного вирішення задачі прихованого передавання інформації. Основною причиною цього є те, що більшість існуючих технологій орієнтована переважно на формування енергетичної або частотної невизначеності, тоді як параметри часової структури сигналу залишаються відносно регулярними.

Це обґрунтовує перспективний напрямок розвитку захищених систем радіозв'язку із застосування таймерних сигнальних конструкцій, які поряд із частотною невизначеністю формують також часову невизначеність сигналу. Поєднання технології ППРЧ з таймерними сигналами створить передумови для одночасного підвищення енергетичної та структурної прихованості передавання, що обумовлює необхідність подальшого дослідження таких методів у наступних розділах дисертаційної роботи. З урахуванням зазначеного обґрунтованим є розроблення широкосмугових сигналів, у яких поєднуються переваги: таймерних сигнальних конструкцій; методів прямого розширення спектра за допомогою псевдовипадкових послідовностей та ППРЧ; комбінованих методів розширення спектра.

Постановка задач дослідження полягає у розробленні методу підвищення прихованості передавання широкосмугових таймерних сигналів на основі ППРЧ, який забезпечуватиме зменшення ймовірності структурного та енергетичного виявлення, підвищення стійкості до завад і радіоелектронного подавлення, а також збереження необхідної пропускної здатності та достовірності передавання інформації в умовах радіоелектронної протидії. На основі зазначеного актуальним напрямом наукового дослідження є:

1) удосконалення моделей формування широкосмугових таймерних сигналів – розробка методів синтезу сигналів із заданими кореляційними та спектральними властивостями для мінімізації ймовірності виявлення.

2) підвищення криптографічної стійкості ППРЧ – дослідження нових генераторів керуючих послідовностей (включно на основі хаотичних систем) та аналіз їх стійкості до прогнозування.

3) інтеграція таймерних сигналів та ППРЧ – дослідження методів розширення спектра, де частотний перескок поєднується з часовою структурою для підвищення структурної невизначеності та стійкості до завад.

4) комбіновані методи розширення спектра – розвиток методів, що інтегрують часові, частотні та структурні принципи кодування для формування складних шумоподібних сигналів.

5) удосконалення методів оцінювання прихованості та завадостійкості – розробка комплексних критеріїв, які враховують ймовірність виявлення, перехоплення, бітову помилковість і пропускну здатність каналу.

Таким чином, подальші дослідження мають бути спрямовані на створення адаптивних, багатофакторних та криптостійких сигнальних конструкцій, зокрема на основі інтеграції таймерних сигналів і ППРЧ, здатних забезпечити високий рівень прихованості та завадозахищеності в умовах сучасної радіоелектронної боротьби.

1.8 Висновки до розділу 1

У першому розділі дисертаційної роботи проведено аналіз особливостей функціонування систем радіозв'язку в умовах радіоелектронної протидії, а також розглянуто основні методи підвищення їх завадозахищеності та прихованості. Встановлено, що сучасне радіоелектронне середовище характеризується високим рівнем активних, пасивних та імітаційних завад, а також широким застосуванням засобів радіорозвідки, що суттєво ускладнює забезпечення стійкого та прихованого передавання інформації.

Проаналізовано вплив радіоелектронної протидії на ключові параметри каналів зв'язку, зокрема відношення сигнал/шум, синхронізацію, ймовірність помилок та пропускну здатність. Показано, що в умовах інтенсивного завадового впливу відбувається комплексна деградація характеристик радіоканалів, що обмежує ефективність класичних методів передавання інформації.

Розглянуто основні методи для підвищення завадозахищеності, включаючи технології розширення спектра, псевдовипадкового перескоку робочої частоти, а також використання широкосмугових і шумоподібних сигналів. Встановлено, що існуючі методи мають обмеження щодо забезпечення одночасно високого рівня прихованості та стійкості до сучасних засобів радіорозвідки.

На основі проведеного аналізу обґрунтовано доцільність подальшого розвитку комбінованих методів передавання інформації, що інтегрують таймерні сигнали та механізми ППРЧ, з метою підвищення структурної невизначеності сигналів та зменшення ймовірності їх виявлення і перехоплення в умовах радіоелектронної протидії.

РОЗДІЛ 2

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА ТА ПСЕВДОВИПАДКОВОГО ПЕРЕСКОКУ РОБОЧОЇ ЧАСТОТИ

У розділі проведено аналіз сучасних методів розширення спектра та їх ролі у забезпеченні захисту інформації в системах радіозв'язку. Розглянуто принципи функціонування та математичні моделі методів прямого розширення спектра псевдовипадковими послідовностями і псевдовипадкового перескоку робочої частоти, визначено їх переваги та обмеження щодо енергетичної, структурної й завадової прихованості. Досліджено комбіновані методи розширення спектра, які поєднують кодове та частотне розосередження сигналу. Обґрунтовано доцільність використання таймерних сигнальних конструкцій як засобу формування додаткової часової невизначеності та підвищення структурної прихованості передавання інформації. Показано, що інтеграція таймерних сигналів із методами ПРС-ПВП та ППРЧ створює теоретичні передумови для побудови комбінованих часово-частотно-кодкових методів захисту інформації.

2.1 Класифікація методів розширення спектра та їх роль у захисті інформації

Розширення спектра є одним із найефективніших методів до захисту інформації в системах радіозв'язку, зокрема в умовах радіоелектронної протидії [33-35]. Цей метод полягає у розподілі енергії сигналу по значно ширшій смузі частот, ніж необхідно для передачі інформації, що ускладнює його виявлення, перехоплення та дешифрування. Залежно від способу реалізації розширення спектра поділяють на ПРС-ПВП, ППРЧ та ППС [38-40]. Кожен із цих методів має свої переваги та обмеження щодо захисту інформації, що визначає їх застосування в різних умовах експлуатації.

Метод ПРС-ПВП базується на модуляції інформаційного сигналу з імпульсами тривалістю t_0 певною псевдовипадковою послідовністю з тривалістю τ , яка має значно вищу швидкість [42,43]

$$V_{\text{пвп}} \gg V_{\text{інф}}, \quad (2.1)$$

ніж інформаційний сигнал $V_{\text{інф}}$. Це дозволяє розподілити енергію сигналу по широкій смузі частот, знижуючи його спектральну густину потужності. Переваги ПРС-ПВП полягають у високій завадостійкості завдяки обробному виграшу, який визначається відношенням ширини спектра після розширення до смуги інформаційного сигналу, а також у стійкості до багатопроменевості. Проте ПРС-ПВП має недоліки: наявність кореляційних ознак, які можуть бути використані засобами радіоелектронної розвідки для виявлення та класифікації сигналів. Крім того, для ефективної роботи ПРС-ПВП потрібна точна синхронізація між передавачем і приймачем, що ускладнює його застосування в умовах динамічної радіоелектронної обстановки.

Метод ППРЧ передбачає періодичну зміну несучої частоти сигналу за псевдовипадковим законом [27,28]. Це дозволяє розподілити енергію сигналу по широкому діапазону частот, знижуючи його спектральну густину потужності. Переваги ППРЧ полягають у високій енергетичній прихованості, оскільки сигнал важко виявити на тлі шуму, а також у стійкості до вузькосмугових завад, оскільки завада впливає лише на невелику частину сигналу. Проте ППРЧ має недоліки: часові параметри стрибків, тривалість перебування на частотній позиції та закономірності синхронізації можуть бути використані для реконструкції структури сигналу, що знижує його структурну прихованість. Крім того, ППРЧ вимагає складнішої апаратної реалізації порівняно з ПРС-ПВП.

Метод ППЧ ґрунтується на зміні моментів передачі імпульсів за псевдовипадковим законом, що створює додаткову часову невизначеність [41]. Переваги ППЧ полягають у підвищенні структурної прихованості, оскільки противнику важко передбачити моменти передачі імпульсів. Проте ППЧ має

недоліки: вимагає високоточної синхронізації та може мати обмежену пропускну здатність через нерегулярність передачі імпульсів.

Порівняння методів розширення спектра з точки зору захисту інформації свідчить про те, що жоден з методів не є універсальним. Метод ПРС-ПВП забезпечує високу завадостійкість та енергетичну прихованість, але має кореляційні ознаки, які можуть бути використані для виявлення сигналу. Метод ППРС забезпечує високу енергетичну прихованість та стійкість до вузькосмугових завад, але має обмежену структурну прихованість [42, 43]. Метод ППЧ [45,46] підвищує структурну прихованість, але вимагає високоточної синхронізації. Обґрунтування доцільності застосування комбінованих способів полягає в тому, що поєднання переваг різних методів дозволяє компенсувати їх недоліки [38-40]. Наприклад, комбінація ПРС-ПВП і ППРС може забезпечити високу завадостійкість, енергетичну та структурну прихованість, а додавання ППЧ дозволяє підвищити часову невизначеність [40]. Такі комбіновані методи є перспективними для сучасних систем радіозв'язку, які повинні функціонувати в умовах інтенсивної радіоелектронної протидії.

2.2 Математичні моделі сигналів з розширеним спектром

Математичні моделі сигналів з розширеним спектром є основою для аналізу їхніх характеристик, оцінки ефективності та розробки методів захисту інформації. Ці моделі дозволяють формалізувати процеси формування сигналів, їхні спектральні та енергетичні властивості, а також оцінити рівень прихованості та завадостійкості [41-44].

Сигнали з ПРС-ПВП формуються шляхом модуляції інформаційного сигналу псевдовипадковою послідовністю, що може подано у вигляді [35, 36]:

$$s_{\text{DSSS}}(t) = A \cdot d(t) \cdot c(t) \cdot \cos(2\pi f_c t), \quad (2.2)$$

де A – амплітуда сигналу, $d(t)$ – інформаційний сигнал (зазвичай двійковий), $c(t)$ – ПВП розширення спектра з швидкістю, значно вищою за швидкість $d(t)$, f_c – несуча частота.

Послідовність $c(t)$ зазвичай формується як ПВП імпульсів з амплітудою ± 1 , яка визначається генератором на основі регістрів зсуву з лінійним зворотним зв'язком. Обробний виграш G_p для ПРС-ПВП [38, 39] визначається як відношення ширини спектра після розширення $B_{\text{ПВП}}$ до смуги інформаційного сигналу B_d (1.42). Цей виграш визначає стійкість ПРС-ПВП до завад та здатність виділяти корисний сигнал на тлі шуму.

Математичний опис сигналів з ППРЧ ґрунтується на періодичній зміні несучої частоти за псевдовипадковим законом та може бути представлений у вигляді [27]:

$$s_{\text{ППРЧ}}(t) = A \cdot d(t) \cdot \cos(2\pi f_i(t)t), \quad (2.3)$$

де $f_i(t)$ – частота на i -му інтервалі, яка визначається псевдовипадковою послідовністю. Частота $f_i(t)$ виражена як (1.38). Середня спектральна густина потужності $S(f)$ для сигналу ППРЧ визначається як (1.39). Модель (1.39) показує, що енергія сигналу розподіляється по широкому діапазону частот, що знижує його спектральну густину потужності та підвищує енергетичну прихованість.

Моделі комбінованих сигналів поєднують переваги обох методів ПРС-ПВП та ППРЧ, забезпечуючи високу завадостійкість та прихованість. Сигнал комбінованого методу може бути поданий у вигляді [34]:

$$s_{\text{комб}}(t) = A \cdot d(t) \cdot c(t) \cdot \cos(2\pi f_i(t)t). \quad (2.4)$$

При цьому методі сигнал спочатку модулюється послідовністю $c(t)$ аналогічно як при ПРС-ПВП, а потім здійснюється псевдовипадковий перескок робочої частоти $f_i(t)$ аналогічно методу ППРЧ. Така комбінація дозволяє: низити спектральну густину потужності завдяки ППРЧ; підвищити завадостійкість

завдяки ППРЧ; ускладнити виявлення та аналіз сигналу завдяки комбінації часової та частотної невизначеності. Отже, комбіновані сигнали є перспективними для сучасних систем радіозв'язку, оскільки вони поєднують переваги обох методів, компенсуючи їхні недоліки.

2.3 Метод прямого розширення спектра для захисту інформації

Метод ПРС-ПВП є одним із найбільш поширених способів формування широкосмугових сигналів для забезпечення завадостійкості та прихованості передавання інформації [39,40]. При розширенні спектра інформаційного сигналу за допомогою ПВП його енергія розподіляється в широкому частотному діапазоні, а спектральна густина потужності зменшується, що ускладнює енергетичне виявлення та підвищує стійкість до навмисних завад.

При цьому методі формування широкосмугового сигналу базується на використанні двох незалежних процесів – інформаційної послідовності та кодової послідовності розширення. Якщо інформаційний сигнал подати у вигляді [43,44]

$$d(t) \in \{-1, +1\}, \quad (2.5)$$

а псевдовипадкову послідовність у вигляді

$$c(t) \in \{-1, +1\}, \quad (2.6)$$

то розширений сигнал формується як

$$s_{DSSS}(t) = A d(t)c(t)\cos(2\pi f_c t + \varphi), \quad (2.7)$$

де A – амплітуда сигналу, f_c – несуча частота, φ – початкова фаза. Отже, кожен інформаційний біт $d(t)$ замінюється набором швидких кодових імпульсів $c(t)$, що

приводить до збільшення смуги сигналу. Коефіцієнт розширення або обробний виграш ПРС-ПВП визначається як [43]

$$G_p = \frac{B_{\text{ПВП}}}{B_d} = \frac{R_c}{R_b}, \quad (2.8)$$

де B_{SS} – ширина спектра після розширення, B_d – смуга інформаційного сигналу, R_c – швидкість ПВП, R_b – швидкість передавання інформації. Збільшення обробного виграшу забезпечує підвищення завадостійкості та зменшення спектральної густини потужності сигналу. У випадку ПРС-ПВП спектральна густина потужності $S(f)$ може бути подана як (1.43). Оскільки після розширення [42,43]

$$B_{\text{ПВП}} \gg B_d, \quad (2.9)$$

то $S(f)$ зменшується і може наближатися до рівня шуму в каналі. Саме ця властивість забезпечує енергетичну прихованість сигналів що сформовані на основі методу ПРС-ПВП. Приймання сигналу в системі ПРС-ПВП базується на виконанні зворотної операції – кореляційного стискання спектра за допомогою синхронізованої копії ПВП. В приймачі виконується множення прийнятого сигналу на локальну кодову послідовність [41]:

$$r(t)c(t) = A d(t)c^2(t) + n(t)c(t), \quad (2.10)$$

де $n(t)$ – шумова складова. Оскільки $c^2(t) = 1$, то корисний сигнал стискається до початкової смуги, тоді як завади та шум залишаються розподіленими у широкому спектрі. У результаті після кореляційної обробки формується обробний виграш (1.35). Ця властивість визначає високу ефективність системи з ПРС-ПВП щодо придушення вузькосмугових та імпульсних завад. В такій системі імовірність помилки приймання для двійкової фазової маніпуляції може оцінюватися через співвідношення [19]

$$P_b = Q\left(\sqrt{2\frac{E_b}{N_0}}\right), \quad (2.11)$$

де $Q(\cdot)$ – функція помилки. При наявності в каналі вузькосмугової завади ефективно співвідношення сигнал/шум після кореляційного стискання збільшується приблизно пропорційно обробному виграшу [33,34]:

$$\left(\frac{S}{N}\right)_{out} \approx G_p \left(\frac{S}{N}\right)_{in}. \quad (2.12)$$

Це пояснює широке застосування методу ПРС-ПВП у системах зв'язку, які працюють в умовах інтенсивної радіоелектронної протидії. Разом із тим ПРС-ПВП має не лише переваги, а й певні обмеження у контексті захисту інформації. До основних переваг належать [36, 43]: зниження спектральної густини потужності та підвищення енергетичної прихованості; високий обробний виграш і стійкість до вузькосмугових та імпульсних завад; можливість кодового розділення каналів для систем CDMA; підвищення завадозахищеності в умовах багатопроменевого поширення.

Однак сучасні засоби радіоелектронної розвідки значною мірою зменшили абсолютні переваги методу ПРС-ПВП. Основним недоліком є необхідність точної синхронізації псевдовипадкових послідовностей у передавачі та приймачі. Порушення синхронізації призводить до втрати кореляційного стискання та різкого погіршення якості зв'язку. Крім того, ПРС-ПВП не забезпечує достатньої структурної прихованості. Після накопичення достатньої кількості спостережень сучасні комплекси радіорозвідки здатні використовувати кореляційні методи пошуку та спектрально-кореляційний аналіз для виявлення ознак ПВП. Імовірність такого виявлення може бути подана як

$$P_{det} = f(T_{obs}, G_p, R_c), \quad (2.13)$$

де T_{obs} – час накопичення. Зі збільшенням часу спостереження та накопичення кореляційної статистики ймовірність виявлення такого сигналу зростає.

Отже, ПРС-ПВП є ефективним методом підвищення енергетичної прихованості та завадозахищеності систем радіозв'язку, однак його можливості щодо забезпечення структурної прихованості є обмеженими. Залежність від кореляційної синхронізації та потенційна можливість статистичного виявлення ПВП сучасними засобами радіорозвідки обмежують перспективи використання ПРС-ПВП як універсального механізму захисту інформації. Це обґрунтовує необхідність подальшого розвитку методів розширення спектра та пошуку алгоритмів, що поєднують частотну й часову невизначеність сигнальних конструкцій.

2.4 Методи псевдовипадкового перескоку робочої частоти

Метод ППРЧ належить до класу технологій розширення спектра та широко застосовується в системах військового і спеціального радіозв'язку для підвищення завадостійкості та прихованості передавання інформації [27-29]. Принцип його функціонування полягає у зміні робочої частоти передавання відповідно до наперед визначеного псевдовипадкового закону, відомого лише легітимним абонентам мережі. У результаті сигнал послідовно переміщується між окремими частотними каналами, що значно ускладнює його виявлення, пеленгування та радіоподавлення.

На відміну від ПРС-ПВП, де розширення спектра реалізується шляхом множення інформаційної послідовності на кодову ПВП, у системах ПРС-ПВП розширення досягається шляхом часово-частотного перескоку робочої частоти. Робоча $f_i = f_{min} + k_i \Delta f$ частота в кожному інтервалі перебування визначається елементом керуючої псевдовипадкової послідовності. Якщо використовується M частотних каналів, то простір можливих частотних позицій визначається як

$$M = \frac{B_{ППРЧ}}{\Delta f}, \quad (2.14)$$

де $B_{\text{ППРЧ}}$ – загальна смуга перебудови. Час перебування на одній частоті визначається параметром T_h , після завершення якого виконується перескок на наступний канал згідно з ПВП. Переданий ППРЧ-сигнал можна представити як

$$s(t) = Ad(t)\cos [2\pi f_i t + \varphi], iT_h \leq t < (i + 1)T_h, \quad (2.15)$$

де $d(t)$ – інформаційна послідовність, A – амплітуда, f_i – частота поточного перескоку. Отже, спектр сигналу в довготривалому інтервалі спостереження займає широку смугу, тоді як у кожен окремий момент часу передавання здійснюється лише у вузькому підканалі. Оскільки енергія сигналу розподіляється між багатьма частотними позиціями, середня спектральна густина потужності $S(f)$ (1.46) зменшується. Зменшення спектральної густини потужності $S(f)$ сприяє підвищенню енергетичної прихованості та ускладнює роботу енергетичних детекторів радіорозвідки. Однією з головних переваг ППРЧ є висока стійкість до навмисних завад. Якщо вузькосмугова завада перекриває лише частину спектра, то її вплив обмежується окремими перескоками. Імовірність ураження одного частотного каналу може бути оцінена як (1.39). Тоді середня частка ушкоджених перескоків визначається саме цією величиною. Чим більша загальна смуга ППРЧ, тим нижча ефективність вузькосмугового подавлення. У разі широкосмугового шумового подавлення ефективність захисту визначається процесом виграшу від перебудови частоти. Для систем FHSS вводиться коефіцієнт обробного виграшу [33]

$$G_{\text{ППРЧ}} = \frac{B_{\text{ППРЧ}}}{B_s}, \quad (2.16)$$

де B_s – смуга інформаційного сигналу. Зростання $G_{\text{ППРЧ}}$ приводить до зменшення ефективності прицільних завад та підвищує завадозахищеність каналу. Ключовим елементом FHSS є псевдовипадкова послідовність, що керує перебудовою частоти. Саме вона визначає структурну прихованість системи та стійкість до

несанкціонованого доступу. Псевдовипадкові послідовності повинні мати великий період, добрі автокореляційні властивості та високу статистичну невизначеність. Період ПВП визначається як [33,34]

$$L_{PN} = 2^n - 1, \quad (2.17)$$

де n – розрядність регістра зсуву.

Для оцінювання кореляційних властивостей використовується автокореляційна функція:

$$R(\tau) = \frac{1}{N} \sum_{i=1}^N c_i c_{i+\tau}, \quad (2.18)$$

де c_i – елементи ПВП. Для якісної послідовності автокореляція повинна мати виражений максимум при $\tau = 0$ та малі бічні пелюстки, що забезпечує точну синхронізацію та низьку ймовірність розкриття структури перебудови.

Кількість можливих частотних маршрутів при довжині послідовності L та числі частот M становить

$$N_{hop} = M^L, \quad (2.19)$$

що демонструє експоненційне зростання складності прогнозування закону перескоку.

У контексті захисту інформації ППРЧ забезпечує три основні механізми: зниження ймовірності енергетичного виявлення завдяки розподілу спектра; підвищення структурної прихованості через невідомий закон перебудови частоти; підвищення стійкості до прицільного радіоподавлення.

Ймовірність успішного перехоплення сигналу без знання ПВП може бути подана як [29,34]

$$P_{int} \approx \frac{1}{M}, \quad (2.20)$$

для одного перескоку, а для серії перескоків

$$P_{int} \approx \left(\frac{1}{M}\right)^L. \quad (2.21)$$

Це пояснює високу ефективність ППРС у військових системах зв'язку. Залежно від співвідношення між швидкістю перескоку та швидкістю передавання інформації розрізняють повільні та швидкі системи ППРС.

У повільних системах з ППРС за час перебування на частоті передається кілька інформаційних символів:

$$T_h > T_s, \quad (2.22)$$

де T_s – тривалість символу. У цьому випадку

$$R_h < R_s, \quad (2.23)$$

де R_h – швидкість перескоків, R_s – швидкість символів. Повільний ППРС характеризується простішою синхронізацією та нижчими вимогами до апаратури, однак окремий канал може залишатися доступним для завад протягом відносно тривалого часу.

У швидких системах перескоки робочої частоти відбуваються частіше, ніж передавання символів, тобто:

$$T_h < T_s, \quad (2.24)$$

або

$$R_h > R_s. \quad (2.25)$$

У цьому випадку один інформаційний символ передається через кілька частотних позицій. Швидкий метод ППРЧ [39,40] забезпечує значно вищу завадостійкість та ускладнює супровід сигналу засобами радіорозвідки, однак вимагає точнішої часової синхронізації та складнішої реалізації.

Окремим напрямом розвитку є багатоканальні системи ППРЧ, у яких одночасно використовуються декілька частотних трактів:

$$N_c > 1. \quad (2.26)$$

Такі системи дозволяють підвищити пропускну здатність та живучість мережі, однак потребують складних алгоритмів керування частотними ресурсами.

Практична реалізація ППРЧ використовується у військових SDR-радіостанціях, системах НАТО HAVE QUICK, SINCGARS, Link-16, а також у сучасних захищених мережах тактичного зв'язку [22,29]. Використання ППРЧ у поєднанні із криптографічним захистом та адаптивним керуванням параметрами передавання дозволяє формувати високостійкі канали зв'язку навіть в умовах інтенсивної радіоелектронної боротьби [40].

Отже, метод ППРЧ є одним із найбільш ефективних способів підвищення прихованості та завадостійкості систем радіозв'язку. Водночас класичні системи ППРЧ не забезпечують повної часової невизначеності, оскільки закон перебудови реалізується переважно у частотній області при відносно регулярній часовій структурі сигналу. Це створює передумови для подальших досліджень, пов'язаних із поєднанням ППРЧ та таймерних сигнальних конструкцій.

2.5 Комбіновані методи розширення спектра

Подальший розвиток засобів радіоелектронної розвідки та радіоелектронного подавлення зумовив необхідність пошуку методів захисту інформації, які б поєднували переваги різних технологій розширення спектра. Окреме використання ПРС-ПВП або ППРЧ забезпечує достатньо високий рівень

завадозахищеності та прихованості, однак кожен із цих методів має власні обмеження. ПРС-ПВП характеризується високим обробним виграшем і низькою спектральною густиною потужності, проте залежить від синхронізації псевдовипадкових послідовностей і може бути виявлений за допомогою кореляційних методів аналізу. Системи ППРЧ, своєю чергою, забезпечують високу стійкість до вузькосмугових завад та ускладнюють перехоплення сигналу, але можуть демонструвати структурну повторюваність часово-частотної перебудови. Це обумовило появу комбінованих методів розширення спектра, у яких одночасно використовуються механізми ПРС-ПВП та ППРЧ.

Інтеграція ПРС-ПВП і ППРЧ [37,39] передбачає формування широкосмугового сигналу, у якому інформаційна послідовність попередньо розширюється кодовою псевдовипадковою послідовністю, а сформований сигнал додатково передається через канал із псевдовипадковим перескоком робочої частоти. Такий підхід дозволяє одночасно реалізувати часово-кореляційне та частотне розширення спектра.

У загальному випадку сигнал на основі ПРС-ПВП формується відповідно до виразу [39]

$$s_{DSSS}(t) = Ad(t)c(t)\cos(2\pi f_c t + \varphi), \quad (2.27)$$

де $d(t)$ – інформаційна послідовність, $c(t)$ – кодова ПВП, f_c – несуча частота.

У комбінованій системі ця несуча частота стає функцією псевдовипадкової перебудови:

$$f_c = f_i(t), \quad (2.28)$$

тому сигнал ПРС-ПВП/ППРЧ набуває вигляду

$$s_{comb}(t) = Ad(t)c(t)\cos[2\pi f_i(t)t + \varphi]. \quad (2.29)$$

У цьому випадку розширення спектра відбувається одразу у двох вимірах – кодовому та частотному. Загальна смуга комбінованого сигналу визначається як

$$B_{comb} \approx B_{DSSS} + B_{FH}, \quad (2.30)$$

де B_{DSSS} – смуга прямого розширення, B_{FH} – смуга частотних перескоків.

Енергетична прихованість такого сигналу додатково підвищується завдяки зменшенню спектральної густини потужності

$$S(f) \approx \frac{P_t}{B_{comb}}, \quad (2.31)$$

де P_t – потужність передавача. Оскільки

$$B_{comb} > B_{DSSS}, \quad (2.32)$$

та

$$B_{comb} > B_{FH}, \quad (2.33)$$

спектральна густина потужності стає нижчою порівняно з окремими методами розширення спектра, що знижує ймовірність енергетичного виявлення сигналу. Обробний виграш комбінованої системи визначається як добуток виграшів окремих методів:

$$G_{comb} = G_{DSSS} \cdot G_{FH}, \quad (2.34)$$

де

$$G_{DSSS} = \frac{R_c}{R_b}, \quad (2.35)$$

$$G_{FH} = \frac{B_{FH}}{B_s}. \quad (2.36)$$

У децибельному вигляді

$$G_{comb}(dB) = G_{DSSS}(dB) + G_{FH}(dB). \quad (2.37)$$

Отже, комбінований підхід забезпечує суттєво більший рівень завадозахищеності, ніж кожен метод окремо.

Особливо важливою перевагою інтегрованих ПРС-ПВП/ППРЧ-систем є підвищення стійкості до різних типів завад. Вузькосмугові прицільні завади ефективно пригнічуються механізмом частотної перебудови, оскільки завада впливає лише на частину перескоків. Водночас шумові широкосмугові завади частково компенсуються завдяки кореляційному стисканню ПРС-ПВП.

Імовірність придушення каналу вузькосмуговою завадою визначається як (1.39). Для комбінованої системи ефективна ймовірність втрати інформації додатково зменшується за рахунок ПРС-ПВП-кореляції [34]:

$$P_{loss} \approx \frac{P_j}{G_{ПВП}}. \quad (2.38)$$

Це свідчить про суттєве підвищення живучості каналу. Ще однією перевагою комбінованих методів є підвищення структурної прихованості. Якщо у класичних ППРЧ-системах після накопичення статистики можливо частково реконструювати закон перебудови частоти, а в системі з ПРС-ПВП – оцінити кореляційні ознаки ПВП, то сумісне використання двох механізмів ускладнює структурний аналіз.

Імовірність правильного структурного виявлення можна умовно подати як

$$P_{str} = P_{ПВП} \cdot P_{ППРЧ}, \quad (2.39)$$

де $P_{ПВП}$ – імовірність розкриття кодової структури, $P_{ППРЧ}$ – імовірність реконструкції закону перескоку. Оскільки обидві події повинні відбутися одночасно, загальна ймовірність структурного розкриття суттєво зменшується.

Порівняно з окремими методами ПРС-ПВП або ППРЧ комбіновані системи мають низку переваг:

- підвищений обробний виграш;
- нижчу спектральну густину потужності;
- більшу стійкість до вузькосмугових і широкосмугових завад;
- зменшену ймовірність енергетичного та структурного виявлення;
- підвищену живучість мережі в умовах РЕБ.

Водночас комбіновані системи на основі ПРС-ПВП та ППРЧ характеризуються й певними обмеженнями. Основними з них є:

- підвищена складність синхронізації;
- збільшені вимоги до швидкодії апаратури;
- складність реалізації алгоритмів генерації та захисту ПВП;
- зростання енергоспоживання SDR-платформ.

Складність синхронізації пояснюється необхідністю одночасного узгодження двох незалежних процесів – кодової послідовності ПРС-ПВП та закону частотних перескоків ППРС. Загальний час входження у зв'язок може бути оцінений як

$$T_{sync} = T_{PN} + T_{hop}, \quad (2.40)$$

де T_{PN} – час кодової синхронізації, T_{hop} – час синхронізації ППРЧ.

Попри ці недоліки, комбіновані методи знайшли практичне застосування у сучасних системах військового та спеціального зв'язку. Це реалізуються у мережах Link-16, HAVE QUICK, сучасних SDR-радіостанціях, системах тактичного обміну даними та окремих мережах супутникового зв'язку. У таких системах ППРС забезпечує кореляційний захист та кодове розділення каналів, тоді як ППРЧ підвищує стійкість до радіоподавлення та ускладнює роботу засобів радіорозвідки.

Разом із тим навіть комбіновані методи розширення спектра на основі ПРС-ПВП та ППРЧ не усувають повністю проблему структурного виявлення, оскільки часові параметри сигналів у більшості випадків залишаються детермінованими. Наявність регулярної часової структури створює можливості для статистичного накопичення та аналізу сигналів сучасними засобами РЕБ. Це формує передумови для подальшого розвитку методів захисту інформації на основі введення додаткової

часової невизначеності, зокрема із використанням таймерних сигнальних конструкцій.

2.6 Обґрунтування використання таймерних сигналів для підвищення прихованості передавання інформації

Подальше вдосконалення методів захисту інформації в системах радіозв'язку пов'язане з необхідністю подолання обмежень класичних технологій розширення спектра. Незважаючи на високу завадозахищеність методів ПРС-ПВП та ППРЧ, їхні сигнали часто характеризуються відносно регулярною часовою структурою, що створює передумови для структурного виявлення засобами радіоелектронної розвідки. Одним із перспективних напрямів підвищення прихованості є використання таймерних сигналів [19, 40-42], у яких інформація кодується не лише амплітудними, фазовими або частотними параметрами, а й часовими інтервалами між елементами сигналу. Такий підхід забезпечує формування додаткової часової невизначеності та розширює можливості захисту інформації.

На відміну від позиційних сигналів [20, 21, 45], де інформація визначається положенням символу у фіксованій часовій сітці, у таймерних сигнальних конструкціях інформаційним параметром виступає тривалість часових інтервалів між імпульсами або фронтами сигналу. Загальна модель таймерного сигналу може бути подана у вигляді [19,43,44,46,47]

$$s(t) = \sum_{i=1}^N a_i p(t - t_i), \quad (2.41)$$

де a_i – амплітуда i -го імпульсу, $p(t)$ – форма елементарного імпульсу, t_i – моменти появи імпульсів. На відміну від класичних схем модуляції, інформація визначається не лише набором амплітуд a_i , а передусім множиною часових позицій

$$T_i = t_{i+1} - t_i. \quad (2.42)$$

Саме міжімпульсні інтервали формують сигнально-кодову конструкцію. У загальному випадку тривалість таймерного інтервалу описується співвідношенням [55]

$$T_i = k_i \Delta + t_0, \quad (2.43)$$

де Δ – базовий часовий крок, n_i – інформаційний параметр, t_0 – опорна тривалість.

Отже, кожна кодова комбінація формується набором часових інтервалів, а не лише послідовністю бітів. Кількість можливих таймерних реалізацій залежить від числа інформаційних відрізків та допустимих часових позицій. Для кодової конструкції довжиною m при числі часових позицій N кількість реалізацій оцінюється комбінаторним виразом [55]

$$N = \frac{u!}{i!(u-i)!}, \quad (2.44)$$

де

$$u = ms - i(s - 1), \quad (2.45)$$

Зі збільшенням N ансамбль можливих сигнальних конструкцій експоненційно зростає, що безпосередньо впливає на структурну прихованість [56,57].

Однією з ключових властивостей ТСК є формування часової невизначеності. Якщо у системах з ППРЧ момент перескоку визначається фіксованим часовим інтервалом

$$T_h = \text{const}, \quad (2.46)$$

то у таймерних сигналах часові позиції можуть змінюватися за псевдовипадковим або інформаційно залежним законом [19]:

$$T_i \neq \text{const}, \quad (2.47)$$

Це означає, що навіть за відомої несучої частоти або закону ППРЧ структура сигналу залишається невизначеною в часовій області. Часова невизначеність може бути оцінена ентропійною мірою [19]:

$$H_T = -\sum_{i=1}^N p_i \log_2 p_i, \quad (2.48)$$

де p_i – імовірність реалізації i -го часового інтервалу. Чим більше значення H_T , тим складніше засобам радіорозвідки реконструювати часову структуру сигналу.

Енергетичний спектр таймерного сигналу суттєво відрізняється від спектра позиційних сигналів. Для довільного набору часових інтервалів спектр сигналу визначається як [19]

$$X(f) = \sum_{i=1}^N a_i P(f) e^{-j2\pi f t_i}, \quad (2.49)$$

де $P(f)$ – спектр одиночного імпульсу. Спектральна густина потужності тоді визначається через [19]

$$S(f) = \lim_{T \rightarrow \infty} \frac{|X_T(f)|^2}{T}, \quad (2.50)$$

Оскільки часові позиції t_i є нерегулярними, спектр ТСК набуває шумоподібного характеру та характеризується менш вираженими дискретними складовими. Це ускладнює спектральне виявлення сигналу. Переваги таймерних сигнальних конструкцій у забезпеченні прихованості визначаються кількома факторами.

По-перше, ТСК забезпечують додаткову часову невизначеність, яка практично відсутня у класичних ПРС-ПВП або ППРЧ. Імовірність правильного структурного виявлення може бути подана як

$$P_{str} = f(T_{obs}, H_T, L_{TSC}), \quad (2.51)$$

де T_{obs} – час спостереження. Зі збільшенням ентропії часової структури та ансамблю сигнальних реалізацій імовірність структурного аналізу зменшується.

По-друге, ТСК формують широкий ансамбль сигнально-кодових конструкцій. Структурна прихованість може бути оцінена через [56,57]

$$S_{стр} = \log_2 N_{ТКС}, \quad (2.52)$$

що узгоджується з раніше введеними показниками прихованості.

По-третє, часове розосередження енергії сприяє зменшенню пікових спектральних компонент, а отже – підвищенню енергетичної прихованості.

Доцільним є інтеграція ТСК із методами розширення спектра [57]. У такому випадку таймерна структура доповнює частотні або кодові механізми захисту.

При інтеграції ТСК з DSSS сигнал набуває вигляду

$$s(t) = \sum_{i=1}^N a_i c_i p(t - t_i) \cos(2\pi f_c t), \quad (2.53)$$

де c_i – елементи ПВП. При цьому розширення спектра досягається одночасно кодовим та часовим механізмами.

У разі інтеграції ТСК із ППРЧ несуча частота стає додатково функцією псевдовипадкового закону перескоку [50,51]:

$$f_i = f_{hop}(i), \quad (2.54)$$

а сигнал описується виразом

$$s_{ТКС-ППРЧ}(t) = \sum_{i=1}^N a_i p(t - t_i) \cos(2\pi f_i t). \quad (2.55)$$

У цьому випадку формується комбінована часово-частотна невизначеність, за якої невідомими залишаються одночасно: момент передавання; частотна позиція; структура сигнально-кової конструкції.

Загальний простір можливих реалізацій комбінованого сигналу може бути оцінений як

$$L_{\text{комб}} = N_{\text{ТКС}} \cdot M^L, \quad (2.56)$$

де M – число частот ППРЧ, L – довжина частотної послідовності. Експоненційне збільшення числа реалізацій суттєво ускладнює роботу засобів РЕР.

Отже, таймерні сигнали створюють додатковий рівень прихованості за рахунок введення часової невизначеності та формування широкого ансамблю сигнально-кових структур. Їх інтеграція з ПРС-ПВП та ППРЧ дозволяє перейти від класичного частотного або кодового розширення спектра до комбінованого часово-частотно-кового методу, що створює теоретичну основу для побудови нових методів захисту інформації в системах військового радіозв'язку.

2.7 Висновки до розділу 2

1. Проведений аналіз методів розширення спектра показав, що технології ПРС-ПВП та ППРЧ забезпечують різні механізми підвищення завадозахищеності й прихованості передавання інформації. Встановлено, що жоден із зазначених методів окремо не забезпечує одночасно високий рівень енергетичної, структурної та часової прихованості, що обґрунтовує доцільність застосування комбінованих методів.

2. Дослідження математичних моделей сигналів з розширеним спектром дозволило формалізувати процеси кодового та частотного розосередження енергії, визначити параметри обробного виграшу та оцінити вплив ширини спектра на енергетичну прихованість сигналів. Показано, що зростання бази сигналу

супроводжується зменшенням спектральної густини потужності та підвищенням стійкості до навмисних завад.

3. Аналіз методу ПРС-ПВП підтвердив його високу ефективність щодо придушення вузькосмугових і широкосмугових завад завдяки кореляційному стисканню спектра та значному обробному вигаду. Водночас встановлено, що наявність кореляційних ознак і залежність від точної кодової синхронізації обмежують структурну прихованість таких сигналів та створюють передумови для їх статистичного виявлення сучасними засобами радіорозвідки.

4. Дослідження методів ППРЧ показало, що псевдовипадкова перебудова робочої частоти забезпечує високу енергетичну прихованість і стійкість до вузькосмугового радіоподавлення. Визначено залежність завадозахищеності від смуги перебудови, швидкості перескоків та кількості частотних позицій. Разом із тим встановлено, що регулярність часової структури класичних систем ППРЧ може використовуватися для часткової реконструкції закону перебудови та знижувати рівень структурної прихованості.

5. Аналіз комбінованих методів на основі ПРС-ПВП та ППРЧ підтвердив доцільність одночасного використання кодового й частотного розширення спектра. Показано, що інтеграція цих методів забезпечує підвищення обробного вигаду, зменшення спектральної густини потужності, збільшення живучості каналу та зниження ймовірності енергетичного й структурного виявлення сигналу порівняно з використанням кожного методу окремо.

6. Обґрунтовано перспективність використання таймерних сигнальних конструкцій для підвищення прихованості передавання інформації. Встановлено, що непозиційний характер ТСК забезпечує формування додаткової часової невизначеності та значне збільшення ансамблю сигнально-кодкових реалізацій. Показано, що інтеграція ТСК з методами ПРС-ПВП і ППРЧ дозволяє перейти від класичного кодового або частотного розширення спектра до комбінованого часово-частотно-кодowego методу, який створює наукове підґрунтя для розробки нових методів захисту інформації в системах радіозв'язку.

Отримані результати формують теоретичне підґрунтя для подальшого розроблення методу підвищення прихованості передавання широкосмугових таймерних сигналів на основі ППРЧ, який розглядається у наступному розділі дисертаційної роботи.

РОЗДІЛ 3

ТАЙМЕРНІ СИГНАЛЬНІ КОНСТРУКЦІЇ ТА ЇХ ВЛАСТИВОСТІ У СИСТЕМАХ ПРИХОВАНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

У розділі досліджено теоретичні засади формування таймерних сигнальних конструкцій як засобу підвищення захищеності інформаційного обміну в інформаційно-комунікаційних системах. Розроблено математичні моделі таймерних сигналів та досліджено закономірності їх формування з урахуванням вимог щодо забезпечення структурної прихованості передавання інформації. Проаналізовано спектральні, автокореляційні та взаємкореляційні характеристики таймерних сигналів, а також особливості їх кореляційного приймання. Встановлено залежності між параметрами таймерного кодування та кількістю можливих сигнально-кодкових реалізацій, що дає змогу оцінювати рівень структурної невизначеності сигналів як показник їх захищеності від виявлення та несанкціонованого перехоплення. Показано, що застосування таймерних сигнальних конструкцій забезпечує формування додаткової часової невизначеності та підвищує структурну прихованість сигналів, створюючи підґрунтя для розроблення методів захисту інформації на фізичному рівні в умовах радіоелектронної протидії.

3.1 Дослідження статистичних і кореляційних властивостей таймерних сигнальних конструкцій для захисту інформації

Одним із перспективних напрямів підвищення прихованості та завадостійкості систем зв'язку є використання таймерних сигналів [19, 38, 47], у яких інформація визначається не тільки амплітудними або частотними параметрами сигналу, а передусім часовою структурою міжсигнальних інтервалів. Такий метод кодування інформації забезпечує додатковий рівень часової

невизначеності, що ускладнює виявлення, класифікацію та структурний аналіз сигналів засобами радіоелектронної розвідки.

Для оцінювання можливостей використання таймерних сигналів доцільно дослідити їх статистичні та кореляційні властивості. Формування таймерних сигналів здійснюється на часовому інтервалі T_c шляхом вибору числа інформаційних часових відрізків m , при якому забезпечується максимальна кількість реалізацій сигнально-кодових конструкцій.

Важливою характеристикою ТСК є коефіцієнт взаємної кореляції між двома довільними кодовими конструкціями довжини n , який визначається як [41]

$$r_{ij} = \frac{\sum_{k=1}^n (x_{ik} - \bar{x}_i)(x_{jk} - \bar{x}_j)}{\sqrt{\sum_{k=1}^n (x_{ik} - \bar{x}_i)^2 \sum_{k=1}^n (x_{jk} - \bar{x}_j)^2}}, \quad (3.1)$$

де x_{ik} , x_{jk} – елементи відповідних сигнальних конструкцій; $\bar{x}_i$, $\bar{x}_j$ – їх середні значення.

Результати розрахунків коефіцієнтів взаємної кореляції та кодових відстаней між окремими ТСК свідчать про значне різноманіття їхніх структурних характеристик. Значення взаємної кореляції змінюються в широких межах – від від’ємних до додатних величин, а кодові відстані характеризуються значним розкидом. Це свідчить про низьку статистичну подібність сигналів та створює передумови для формування ефективних алгоритмів каналного кодування і розпізнавання.

Для аналізу властивостей таймерних сигналів використовується автокореляційна функція (АКФ), яка визначається як [42]

$$R(\tau) = \sum_{i=1}^N x_i(t)x_i(t + \tau), \quad (3.2)$$

де N – число часових елементів конструкції; τ – часове зміщення.

Для порівняльного аналізу доцільно застосовувати нормовану автокореляційну функцію [41]

$$r(\tau) = \frac{R(\tau)}{R(0)} \quad (3.3)$$

Наведені залежності демонструють характерну для ТСК властивість – наявність вузького центрального максимуму та порівняно низьких бічних пелюсток. Це означає, що сигнал має добрі часові селекційні властивості та може бути ефективно виділений у приймачі при мінімальному рівні міжсимвольних завад.

Важливим для систем прихованого зв'язку є дослідження взаємнокореляційних властивостей таймерних сигналів. Взаємнокореляційна функція (ВКФ) визначається як

$$R_{ij}(\tau) = \sum_{k=1}^N x_i(k)x_j(k+\tau), \quad (3.4)$$

а її нормована форма –

$$r_{ij}(\tau) = \frac{R_{ij}(\tau)}{\sqrt{R_i(0)R_j(0)}}, \quad (3.5)$$

Дослідження ВКФ показує ТСК, що максимальні бічні викиди між різними ТСК не перевищують порівняно малих значень, що підтверджує низький рівень взаємної кореляції між сигналами. Графіки нормованих АКФ таймерних сигналів, наданих на рис. 3.1 – 3.4, підтверджують, що різні сигнальні конструкції (ТСК1, ТСК2, ТСК3, ТСК4) характеризуються відмінною формою кореляційних залежностей. Це має принципове значення для систем прихованого передавання інформації, оскільки відсутність регулярної структури та різноманітність АКФ ускладнюють роботу кореляційних та енергетичних детекторів радіоелектронної розвідки.

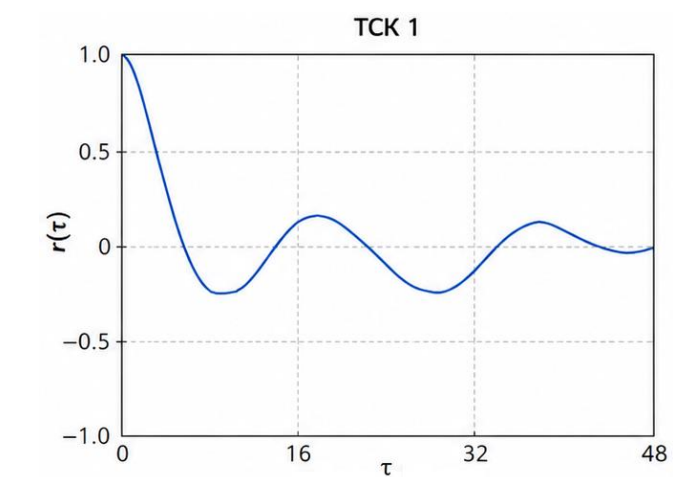


Рис. 3.1. Графік нормованої АКФ таймерного сигналу ТСК1

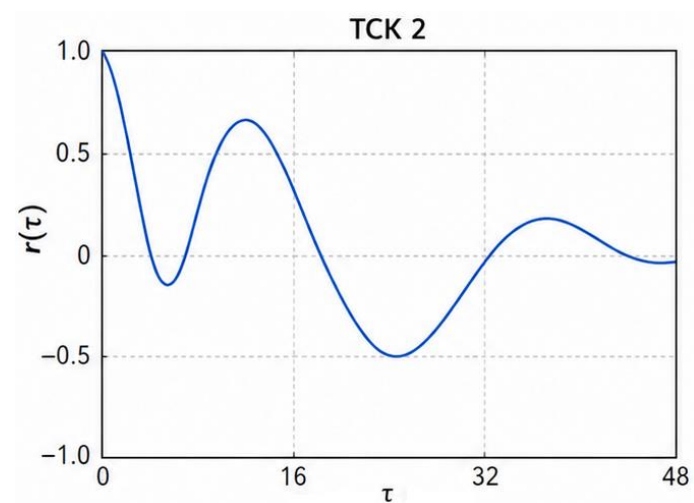


Рис. 3.2. Графік нормованої АКФ таймерного сигналу ТСК2

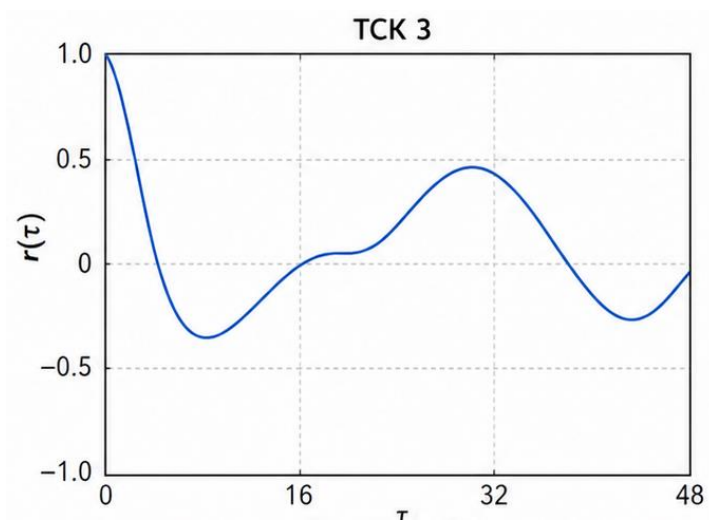


Рис. 3.3. Графік нормованої АКФ таймерного сигналу ТСК3

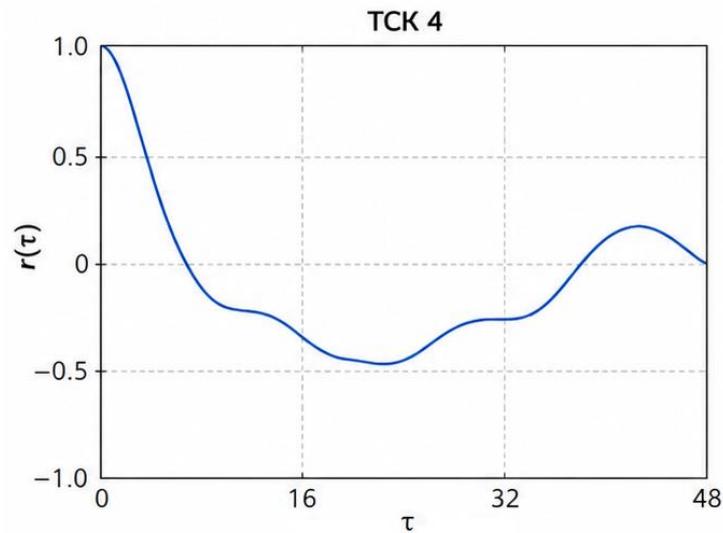


Рис. 3.4. Графік нормованої АКФ таймерного сигналу ТСК4

На рис. 3.5 надано приклади побудови таймерних сигналів на інтервалі часу T_c з параметрами: m , s , Δ та i , де:

- 1) $m = 4$ – кількість елементів на інтервалі Найквіста t_0 ;
- 2) $s = 4$ – кількість часових інтервалів Δ на інтервалі часу $t_0 = s \times \Delta$;
- 3) $i = 2$ – кількість значущих моментів модуляції (ЗММ).

Отже, непозиційні ТСК на відміну від позиційних розрядно-цифрових кодів (РЦК) синтезуються на часовому інтервалі $T_c = mt_0$ [19, 47]. Значення базовий часового інтервалу Δ залежить s і визначається співвідношенням $\Delta = t_0/s$.

В таймерних сигналах алгоритм формування сигнальних конструкцій на відміну від позиційних кодів відрізняється, що пов'язано з тим, що тривалість імпульсів в межах комбінації може змінюватися з урахуванням наступного правила:

$$t_c = t_0 + k\Delta, \quad (3.6)$$

де $k = 0, 1, 2, \dots, s(m-2)$. Отже, тривалість імпульсу t_c буде не менше інтервалу Найквіста t_0 . В результаті формування реалізацій ТСК кожна її комбінація буде визначатися певної структурою часових позицій імпульсів t_c на інтервалі часу T_c . Це забезпечує унікальність кожної комбінації ТСК. Таймерні сигнали, що

представлені на рис. 3.5 під різними номерами, мають певні свої тривалості імпульсів t_c в межах інтервалу T_c :

- 1) $t_{c1} = 4\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 8\Delta$;
- 2) $t_{c1} = 4\Delta$; $t_{c2} = 5\Delta$; $t_{c3} = 7\Delta$;
- 3) $t_{c1} = 4\Delta$; $t_{c2} = 6\Delta$; $t_{c3} = 6\Delta$;
- 4) $t_{c1} = 4\Delta$; $t_{c2} = 7\Delta$; $t_{c3} = 5\Delta$;
- 5) $t_{c1} = 4\Delta$; $t_{c2} = 8\Delta$; $t_{c3} = 4\Delta$;
- 6) $t_{c1} = 5\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 7\Delta$;
- 7) $t_{c1} = 5\Delta$; $t_{c2} = 5\Delta$; $t_{c3} = 6\Delta$;
- 8) $t_{c1} = 5\Delta$; $t_{c2} = 6\Delta$; $t_{c3} = 5\Delta$;
- 9) $t_{c1} = 5\Delta$; $t_{c2} = 7\Delta$; $t_{c3} = 4\Delta$;
- 10) $t_{c1} = 6\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 6\Delta$;
- 11) $t_{c1} = 6\Delta$; $t_{c2} = 5\Delta$; $t_{c3} = 5\Delta$;
- 12) $t_{c1} = 6\Delta$; $t_{c2} = 6\Delta$; $t_{c3} = 4\Delta$;
- 13) $t_{c1} = 7\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 5\Delta$;
- 14) $t_{c1} = 7\Delta$; $t_{c2} = 5\Delta$; $t_{c3} = 4\Delta$;
- 15) $t_{c1} = 8\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 4\Delta$.

Такі унікальні часові особливості побудови кожної комбінації ТСК є основою для створення певного рівня їх невизначеності для стороннього спостерігача, що ускладнює процедуру їх розпізнавання у випадку перехоплення повідомлення. За рахунок такого алгоритму формування таймерні сигнали у порівнянні з РЦК дозволяють збільшити кількість реалізацій на інтервалу часу T_c [19, 53]:

$$N_{\text{тск}} = \frac{[ms-(s-1)i]!}{i!([ms-(s-1)i]-i)!}. \quad (3.7)$$

Для РЦК кількість реалізацій визначається як [19]

$$N = 2^m, \quad (3.8)$$

що для $m = 4$ можна сформувати усього 16 комбінацій. На цьому ж інтервалі для ТСК можна сформувати згідно (3.9) 45 таймерних конструкцій.

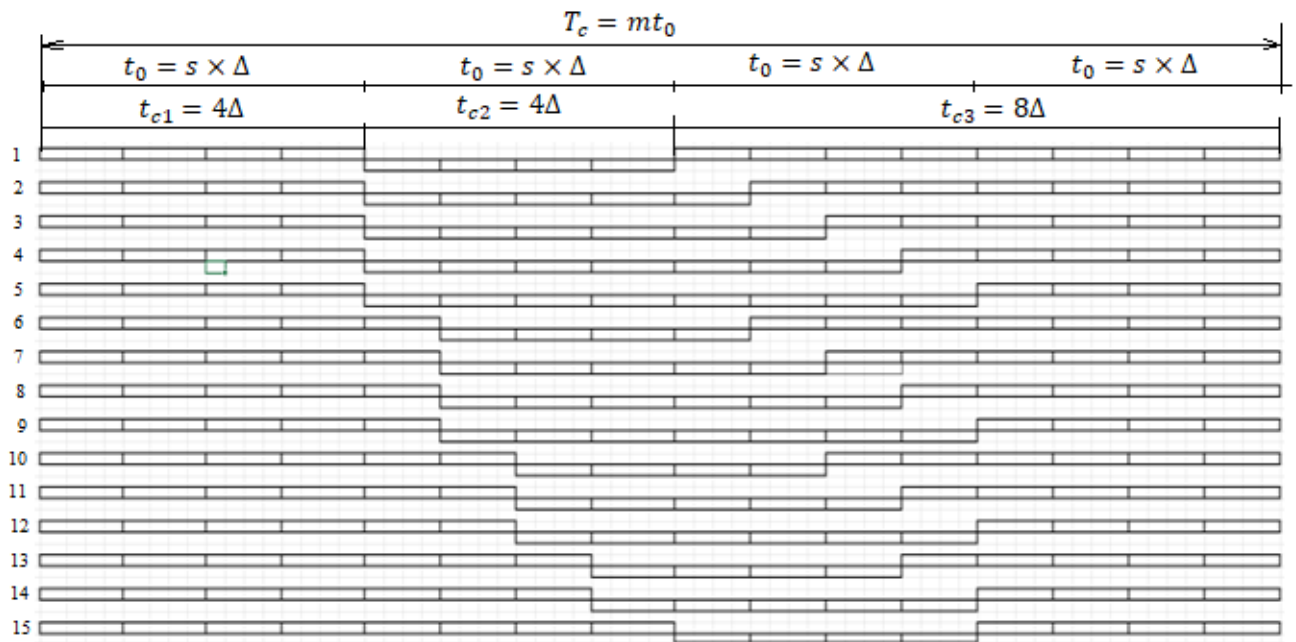


Рис. 3.5. Приклади побудови 15 таймерних сигналів на інтервалі часу T_c з параметрами: $m = 4$, $s = 4$, $\Delta = t_0/4$ та $i=2$

Розглянемо поняття кодової відстані для таймерних сигналів. На відміну від класичних позиційних кодів [19], де кодова відстань зазвичай визначається кількістю різних бітових позицій (відстань Хеммінга), для таймерних сигнальних конструкцій вона характеризує відмінності саме в часовому розташуванні інформаційних елементів Δ . Тому кодова відстань є важливим показником структурної подібності або відмінності таймерних сигналів та безпосередньо впливає на їх кореляційні властивості. Отже, кодова відстань для таймерних сигналів визначається через суму відхилень відповідних часових інтервалів, виражених у елементарних часових відрізках Δ . Якщо два таймерні сигнали описуються наборами часових інтервалів

$$S_i = \{t_{i1}, t_{i2}, \dots, t_{in}\},$$

$$S_j = \{t_{j1}, t_{j2}, \dots, t_{jn}\},$$

то кодова відстань між ними може бути визначена як

$$d_{ij}(\Delta) = \sum_{k=1}^n \left| \frac{t_{ik} - t_{jk}}{\Delta} \right|. \quad (3.9)$$

де $d_{ij}(\Delta)$ – кодова відстань між таймерними сигналами S_i та S_j ; t_{ik}, t_{jk} – тривалості відповідних часових інтервалів сигналів; Δ – мінімальний часовий квант (роздільна здатність таймерного кодування); n – кількість інформаційних інтервалів у сигналі.

В табл. 3.1 та 3.2 кодова відстань фактично показує кількість елементів Δ , на які відрізняються дві сигнальні конструкції, тобто:

$$d_{ij}(\Delta) = N_{\Delta}, \quad (3.10)$$

де N_{Δ} – кількість часових позицій або інтервалів, що відрізняються між двома ТСК. Для наведених у табл. 3.1 результатів:

$$d_{12} = 1\Delta, d_{13} = 2\Delta, d_{15} = 4\Delta,$$

що означає, що структура сигналу №2 відрізняється від сигналу №1 на один часовий квант, сигнал №3 – на два Δ , а сигнал №5 – на чотири Δ .

У проведених дослідженнях кодова відстань оцінювалася в одиницях елементарного інтервалу Δ та характеризувала кількість часових елементів, якими відрізняються дві ТСК. Чим більше значення $d_{ij}(\Delta)$, тим меншою є структурна подібність сигналів і, як правило, меншим є коефіцієнт їх взаємної кореляції.

В табл. 3.1 та 3.2 надано парні коефіцієнти кореляції між 15 таймерними сигналами r_{ij} . Аналіз даних таблиці показує, що між кодовою відстанню та коефіцієнтом взаємної кореляції існує виражена обернена залежність. Для сигналів, які відрізняються лише на один елемент Δ , коефіцієнти кореляції знаходяться в межах $r = 0,856 - 0,882$. Наприклад, для пари сигналів №4 і №5 при кодовій відстані $d_{\min} = 1\Delta$ коефіцієнт взаємної кореляції становить $r = 0,882$, що свідчить про високу структурну схожість сигналів.

При збільшенні кодової відстані до 2Δ значення коефіцієнтів кореляції зменшуються до рівня $0,709 - 0,775$, а для відстані 3Δ становлять переважно

0,545 – 0,674. Подальше збільшення кодової відстані до 4Δ призводить до зниження коефіцієнтів взаємної кореляції до значень близько 0,577 – 0,655.

Для сигналів із кодовою відстанню $5\Delta - 6\Delta$ коефіцієнти кореляції зменшуються до 0,149 – 0,493, що свідчить про суттєве зниження структурної подібності. Так, для пари сигналів №1 і №12 при кодовій відстані 6Δ коефіцієнт кореляції становить лише $r = 0,149$, а для пари №1 і №13 при тій самій відстані отримано $r = 0$, що відповідає практично повній відсутності кореляційного зв'язку між сигналами.

Найменші значення кореляції спостерігаються при кодових відстанях $7\Delta - 8\Delta$. Зокрема, для пари сигналів №2 і №15 при $d_{\min} = 7\Delta$ коефіцієнт кореляції становить $r = -0,078$, що свідчить про практично повну структурну незалежність сигналів.

Отримані результати підтверджують, що збільшення кодової відстані між таймерними сигнальними конструкціями приводить до зменшення їх взаємної кореляції. Це є важливою властивістю ТСК, оскільки дозволяє формувати ансамблі сигналів із низьким рівнем взаємної кореляції, що підвищує їх шумоподібність, структурну прихованість та стійкість до виявлення засобами радіоелектронної розвідки. Крім того, кодова відстань може використовуватися як критерій синтезу оптимальних ансамблів таймерних сигнальних конструкцій із заданими кореляційними характеристиками для систем захищеного радіозв'язку.

Для кількісного оцінювання кореляційних властивостей ансамблю таймерних сигналів доцільно використовувати середній коефіцієнт взаємної кореляції, який дозволяє оцінити загальний рівень статистичної подібності сигналів та ступінь їх взаємної незалежності.

Для ансамблю з N таймерних сигнальних конструкцій середній коефіцієнт взаємної кореляції визначається як [41]

$$\bar{r} = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^N r_{ij}, \quad (3.11)$$

де r_{ij} – коефіцієнт взаємної кореляції між i -ю та j -ю таймерними сигналами, а N – кількість ТСК в ансамблі.

Таблиця 3.1

Парні коефіцієнти кореляції та кодова відстань $d(\Delta)$ між таймерними сигналами r_{ij} під номерами 1-8

	1	2	3	4	5	6	7	8
1	1.000 (0)	0.856 (1)	0.745 (2)	0.655 (3)	0.577 (4)	0.667 (2)	0.545 (3)	0.655 (4)
2	0.856 (1)	1.000 (0)	0.870 (1)	0.764 (2)	0.674 (3)	0.856 (1)	0.709 (2)	0.592 (3)
3	0.745 (2)	0.870 (1)	1.000 (0)	0.878 (2)	0.775 (2)	0.745 (2)	0.870 (1)	0.733 (2)
4	0.655 (3)	0.764 (2)	0.878 (1)	1.000 (0)	0.882 (1)	0.655 (3)	0.764 (2)	0.878 (1)
5	0.577 (4)	0.674 (3)	0.775 (2)	0.882 (1)	1.000 (0)	0.577 (4)	0.674 (3)	0.775 (2)
6	0.667 (2)	0.856 (1)	0.745 (2)	0.655 (3)	0.577 (4)	1.000 (0)	0.856 (1)	0.745 (2)
7	0.545 (3)	0.709 (2)	0.870 (1)	0.764 (2)	0.674 (3)	0.856 (1)	1.000 (0)	0.870 (1)
8	0.655 (4)	0.592 (3)	0.733 (2)	0.878 (1)	0.775 (2)	0.745 (2)	0.870 (1)	1.000 (0)
9	0.364 (5)	0.493 (4)	0.618 (3)	0.746 (2)	0.882 (1)	0.655 (3)	0.764 (2)	0.878 (1)
10	0.333 (4)	0.545 (3)	0.745 (2)	0.655 (3)	0.577 (3)	0.856 (2)	0.856 (1)	0.745 (2)
11	0.234 (5)	0.418 (4)	0.592 (3)	0.764 (2)	0.674 (3)	0.745 (3)	0.709 (2)	0.870 (1)
12	0.149 (6)	0.313 (5)	0.467 (4)	0.618 (3)	0.775 (2)	0.655 (4)	0.591 (3)	0.733 (2)
13	0.000 (6)	0.234 (5)	0.447 (4)	0.655 (3)	0.577 (4)	0.333 (4)	0.545 (3)	0.745 (2)
14	0.078 (7)	0.127 (6)	0.313 (5)	0.493 (4)	0.674 (3)	0.233 (5)	0.418 (4)	0.592 (3)
15	0.333 (8)	-0.078 (7)	0.149 (6)	0.364 (5)	0.577 (4)	0.000 (6)	0.233 (5)	0.447 (4)

Таблиця 3.2

Парні коефіцієнти кореляції між таймерними сигналами r_{ij} під номерами 9-15

	9	10	11	12	13	14	15
1	0.364	0.333	0.234	0.149	0.000	.078	0.333
2	0.493	0.545	0.418	0.313	0.234	0.127	0.078
3	0.618	0.745	0.592	0.467	0.447	0.364	0.149
4	0.746	0.655	0.764	0.618	0.655	0.493	0.364
5	0.882	0.577	0.674	0.775	0.577	0.674	0.577
6	0.655	0.856	0.745	0.655	0.577	0.000	0.870
7	0.764	0.674	0.545	0.709	0.870	0.764	0.674
8	0.746	0.878	0.775	0.733	0.878	0.745	0.745
9	1.000	0.882	0.764	0.746	0.655	0.364	0.618
10	0.882	1.000	0.856	0.745	0.655	0.577	0.667
11	0.764	0.856	1.000	0.870	0.764	0.674	0.545
12	0.746	0.745	0.870	1.000	0.878	0.745	0.870
13	0.655	0.667	0.856	0.745	1.000	0.856	0.745
14	0.764	0.545	0.709	0.870	0.856	1.000	0.870
15	0.618	0.333	0.545	0.745	0.666	0.856	1.000

Для досліджуваного набору з $N = 15$ сигнальних конструкцій кількість унікальних пар становить $M = N(N - 1)/2 = 105$. Після підсумовування всіх позадіагональних елементів матриці взаємної кореляції отримано сумарне значення $\sum r_{ij} = 67,158$, що дозволило визначити середній коефіцієнт взаємної кореляції ансамблю $\bar{r} \approx 0,64$. Отримане значення характеризує ансамбль таймерних сигнальних конструкцій як помірно корельований. Для ідеально ортогонального ансамблю взаємні коефіцієнти кореляції між різними сигналами повинні прямувати до нуля,

$$r_{ij} \rightarrow 0, i \neq j, \quad (3.12)$$

що відповідає умові $\bar{r} \rightarrow 0$. У протилежному випадку, коли сигнали є практично ідентичними, $r_{ij} \rightarrow 1$, середній коефіцієнт взаємної кореляції також наближається до одиниці. Отже, величина $\bar{r}$ є інтегральною характеристикою ансамблю, яка показує ступінь його статистичної однорідності. Для більш наочного оцінювання взаємної незалежності сигналів доцільно ввести коефіцієнт ортогональності ансамблю

$$K_{\text{орт}} = 1 - \bar{r}. \quad (3.13)$$

Для досліджуваного ансамблю ТСК його значення становить $K_{\text{орт}} = 0,36$. Фізичний зміст цього параметра полягає у визначенні ступеня близькості ансамблю до ортогонального простору сигналів. У випадку повної ортогональності $K_{\text{орт}} = 1$, тоді як для повністю подібних або сильно корельованих сигналів $K_{\text{орт}} \rightarrow 0$.

Отримане значення $K_{\text{орт}} = 0,36$ свідчить про те, що досліджуваний ансамбль ТСК не є ортогональним, однак характеризується помірним рівнем взаємної незалежності. Це означає, що в ансамблі присутні як сигнали з високим ступенем подібності, так і слабкорельовані або практично незалежні сигнальні конструкції. Зокрема, у матриці взаємної кореляції табл. 3.1 та 3.2 спостерігаються пари

сигналів із близькими до нуля коефіцієнтами взаємної кореляції, що вказує на можливість формування слабкорельованих підмножин ТСК. Такі результати мають важливе практичне значення при формуванні шумоподібних сигналів на основі таймерних конструкцій. Відомо, що рівень взаємної кореляції між елементами ансамблю визначає форму автокореляційних та взаємно-кореляційних функцій результуючого широкосмугового сигналу, а також впливає на рівень міжсигнальних завад. При відносно високих значеннях взаємної кореляції можуть виникати бічні кореляційні максимуми, що ускладнює процес кореляційного приймання та може збільшувати ймовірність помилкової ідентифікації сигналу. Це означає, що для позиційних сигналів алгоритм кореляційного приймання сигнальної конструкції повинен відрізнятися від позиційних кодів. Водночас наявність слабкорельованих ТСК забезпечує формування широкосмугових сигналів із більш рівномірним спектральним розподілом енергії та підвищеною структурною прихованістю.

Отже, значення коефіцієнта ортогональності $K_{\text{орт}} = 0,36$ підтверджує придатність досліджуваного ансамблю таймерних сигналів для формування шумоподібних сигналів, хоча одночасно вказує на доцільність подальшої оптимізації ансамблю шляхом відбору слабкорельованих ТСК. Зменшення середнього коефіцієнта взаємної кореляції дозволить підвищити ортогональність ансамблю, знизити рівень міжсигнальних завад та покращити завадозахищеність і прихованість систем передавання інформації.

Аналіз кореляційних властивостей ТСК показує, що їх відмінність одна від одної дозволяє реалізувати прийом сигналів у цілому. У цьому випадку вся інформація, що міститься у прийнятому сигналі, використовується єдиною вирішальною схемою при декодуванні, що забезпечує підвищення достовірності приймання та завадостійкості системи.

З точки зору прихованості передавання інформації використання таймерних сигналів [44, 47, 49-52] має низку переваг порівняно з класичними позиційними сигналами. По-перше, часове кодування створює додаткову структурну невизначеність, що ускладнює класифікацію сигналів. По-друге, низькі рівні

взаємної кореляції між ТСК зменшують ймовірність їх виявлення та перехоплення. По-третє, можливість інтеграції ТСК із методами розширення спектра та ППРЧ формує багатовимірний простір сигнально-кодових реалізацій, що підвищує загальний рівень прихованості системи.

Отже, дослідження статистичних і кореляційних властивостей таймерних сигнальних конструкцій підтверджує доцільність їх використання як основи для побудови систем прихованого та завадозахищеного радіозв'язку. Сукупність часової невизначеності, низьких кореляційних властивостей та великого ансамблю можливих реалізацій створює передумови для підвищення енергетичної та структурної прихованості передавання інформації.

3.2 Вплив кореляційних властивостей таймерних сигналів на формування шумоподібних сигналів

Кореляційні властивості таймерних сигналів суттєво впливають на можливість формування шумоподібних сигналів та визначають їх прихованість, завадостійкість і селективні властивості [44, 46, 47]. При використанні ТСК як базових сигнальних елементів широкосмугових систем зв'язку взаємна кореляція між окремими конструкціями визначає рівень міжсигнальних завад, а форма автокореляційної функції – точність часової синхронізації та якість кореляційного приймання.

При формуванні шумоподібного сигналу на основі ансамблю таймерних конструкцій результуючий сигнал може бути поданий у вигляді

$$s(t) = \sum_{i=1}^N a_i s_i(t), \quad (3.14)$$

де $s_i(t)$ – окремі таймерні сигнали, a_i – вагові коефіцієнти або керуюча послідовність, N – число використовуваних ТСК.

Кореляційні характеристики такого сигналу визначаються сукупністю автокореляційних та взаємно-кореляційних властивостей складових сигналів. Автокореляційна функція результуючого ШПС має вигляд [41]

$$R_s(\tau) = \int s(t)s(t - \tau) dt. \quad (3.15)$$

Для ефективного шумоподібного сигналу бажаною є форма АКФ із вузьким головним пелюстком і низькими бічними максимумами:

$$R_s(\tau) \rightarrow \begin{cases} R_s(0), & \tau = 0, \\ \approx 0, & \tau \neq 0. \end{cases} \quad (3.16)$$

Саме така форма забезпечує високу часову локалізацію енергії та підвищує точність кореляційного виявлення. Матриця коефіцієнтів взаємної кореляції (табл. 3.1) показала, що частина ТСК має низькі або близькі до нуля значення $r_{ij} \approx 0$, тоді як інші – помірні та високі значення $r_{ij} = 0.7\text{--}0.88$. Це безпосередньо впливає на якість формування шумоподібних сигналів. Для ансамблю ТСК середній рівень міжсигнальної кореляції можна оцінити як

$$\bar{r} = \frac{2}{N(N-1)} \sum_{i < j} r_{ij}. \quad (3.17)$$

Чим менше значення $\bar{r}$, тим ближче ансамбль до ортогонального та тим кращими є шумоподібні властивості сформованого сигналу. Низькі значення взаємної кореляції забезпечують: зменшення міжканальних завад; підвищення роздільної здатності кореляційного приймача; зниження ймовірності хибного розпізнавання; формування більш рівномірного енергетичного спектра.

Нерівномірний кореляційний простір ТСК формує додаткову часову та структурну невизначеність. Якщо для класичних ПРС-ПВП або ППРЧ структура псевдовипадкової послідовності [44, 48, 57, 61] найчастіше описується відомими

моделями, то для таймерних сигналів структура визначається часовими інтервалами між інформаційними елементами.

Ймовірність структурного розкриття може бути пов'язана з кількістю допустимих конструкцій $L_{ТСК}$ через

$$P_{\text{стр}} \sim \frac{1}{L_{ТСК}}. \quad (3.18)$$

Отримані кореляційні характеристики свідчать, що таймерні сигнали можуть використовуватись як ефективна основа для формування шумоподібних сигналів. Наявність слабокорельованих та практично ортогональних ТСК з різними значенням забезпечує формування широкосмтових сигналів із низьким рівнем бічних кореляційних максимумів, рівномірним спектральним розподілом енергії та підвищеною структурною прихованістю. Це створює передумови для побудови нових методів захисту інформації, у яких шумоподібність досягається не лише псевдовипадковим керуванням частотою або фазою, а й часовою структурою самих сигнальних конструкцій.

3.3 Аналіз кореляційного приймання позиційних та непозиційних шумоподібних сигналів

Базовим методом виявлення цифрових сигналів у системах зв'язку є кореляційне приймання [33, 34, 41], яке забезпечує максимальне відношення сигнал/шум у каналах із адитивним білим гаусівським шумом. Суть кореляційного приймання полягає у визначенні ступеня подібності між прийнятим сигналом та еталонною сигнальною реалізацією, яка формується у приймачі.

Нехай прийнятий сигнал має вигляд [40, 41]

$$r(t) = s(t) + n(t), \quad (3.19)$$

де $s(t)$ – корисний сигнал, $n(t)$ – шумова складова. Тоді вихід корелятора визначається інтегралом

$$Z = \int_0^T r(t) s_0(t) dt, \quad (3.20)$$

де $s_0(t)$ – опорний (еталонний) сигнал, T – інтервал спостереження. Максимальне значення Z відповідає найбільшій подібності між прийнятим та опорним сигналами.

Для позиційних сигналів значущі моменти модуляції жорстко прив'язані до інтервалу Найквіста t_0 . Тому процес кореляційного приймання реалізується шляхом порівняння прийнятого сигналу з набором стандартних еталонних реалізацій. Для двох позиційних сигналів $s_1(t)$ та $s_2(t)$ взаємна кореляційна функція визначається як [33,34]

$$R_{12}(\tau) = \int_0^T s_1(t) s_2(t - \tau) dt. \quad (3.21)$$

Автокореляційна функція має вигляд згідно (3.15). Для позиційних кодів характерним є вузький головний максимум автокореляційної функції та відносно високі бічні пелюстки, величина яких визначається структурою кодової послідовності. Перевагою позиційних сигналів є простота синхронізації та реалізації кореляційного приймача, оскільки моменти прийняття рішення заздалегідь визначені.

На рис. 3.6 представлено процес кореляційного приймання шумоподібного сигналу, сформованого на основі позиційної псевдовипадкової послідовності. У таких системах передавання інформації кожен інформаційний символ розширюється кодовою послідовністю, а приймання здійснюється методом кореляційної обробки з використанням локально сформованого опорного сигналу.

Принцип роботи приймача полягає у перемноженні прийнятого шумоподібного сигналу з опорною псевдовипадковою послідовністю та

подальшому інтегруванні отриманого результату на інтервалі символу t_0 . Вихід кореляційного перемножувача визначається виразом [36, 37]

$$u_m(t) = r(t) \times c(t), \quad (3.22)$$

де $r(t)$ – прийнятий шумоподібний сигнал, $c(t)$ – локальна опорна псевдовипадкова послідовність.

Подальше накопичення результатів перемноження в інтеграторі описується залежністю [33, 34]

$$U_{\text{інт}} = \int_0^{t_0} r(t)c(t) dt. \quad (3.23)$$

Величина $U_{\text{інт}}$ характеризує ступінь кореляційного збігу між прийнятим та опорним сигналами. Якщо послідовності синхронізовані та їх структура збігається, результати перемноження мають переважно однаковий знак, що забезпечує накопичення позитивної енергії та формування кореляційного максимуму U_{max} . У випадку антикореляції або відсутності синхронізації інтегратор накопичує від'ємні складові, що приводить до формування мінімального значення $-U_{\text{min}}$. Для прийняття рішення використовуються порогові рівні $\pm \frac{U_{\text{max}}}{2}$, які визначають область достовірного виявлення переданого символу.

На рис. 3.6 (а) представлений графік широкосмугового дискретного сигналу, поновлений після демодуляції. Результати перемноження прийнятого та опорного сигналів відображає графік на рис. 3.6 (б). Окремі прямокутні елементи відповідають добуткам кодових символів ПВП та мають позитивний або негативний знак залежно від ступеня їх відповідності. Графік на рис. 3.6 (в) демонструє роботу інтегратора, який здійснює накопичення цих значень у межах часового інтервалу t_0 . У першому та третьому інтервалах спостерігається впевнене накопичення позитивної енергії, що свідчить про правильний кореляційний збіг сигналів і формування максимального вихідного рівня. У другому та четвертому

інтервалах відбувається накопичення негативних складових, що відповідає частковому або повному розузгодженню сигналів та приводить до зниження інтегральної напруги.

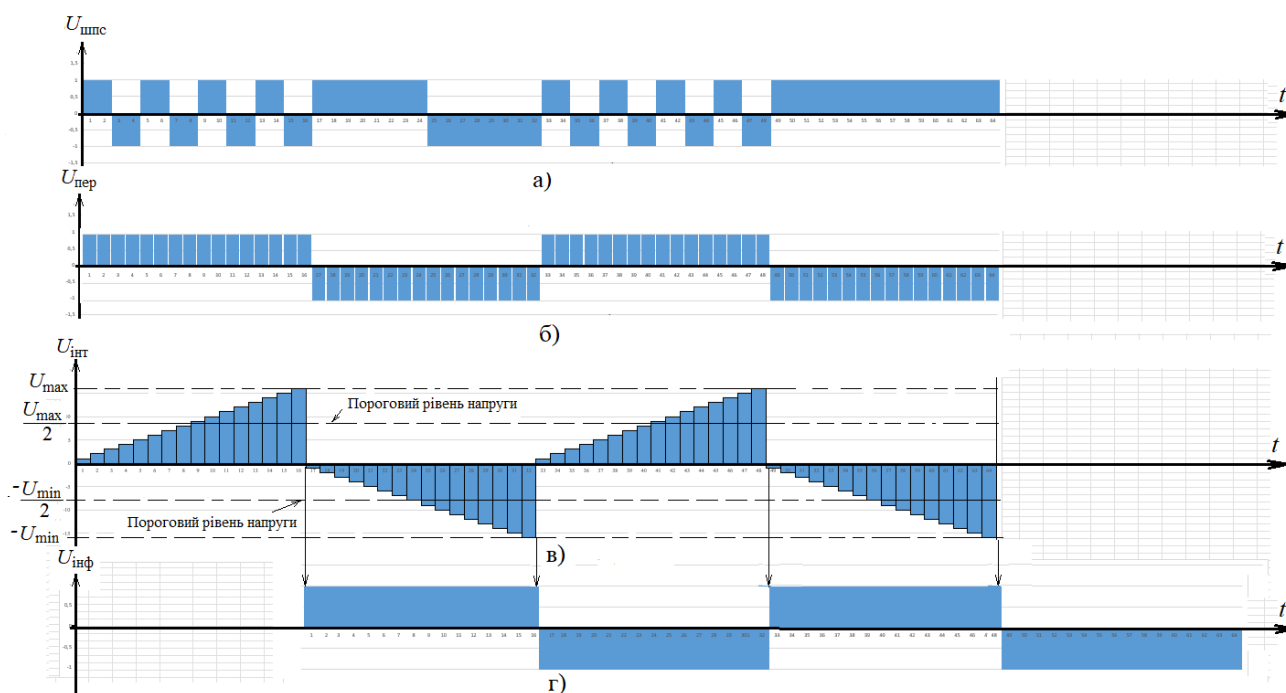


Рис. 3.6. Кореляційне приймання позиційного шумоподібного сигналу

Особливістю позиційного шумоподібного сигналу є те, що процес приймання безпосередньо залежить від правильного відтворення ПВП та забезпечення часової синхронізації. При втраті синхронізму кореляційний максимум різко зменшується, а рівень накопиченої напруги може не перевищувати порогового значення. Отже, ефективність кореляційного приймання позиційних шумоподібних сигналів визначається якістю синхронізації та точністю відтворення кодової структури сигналу.

Порівняно з шумоподібними таймерними сигналами, у позиційних системах кореляційне накопичення базується переважно на збігу кодових елементів ПВП, тоді як часова структура сигналу залишається фіксованою. Це спрощує процедуру синхронізації, однак одночасно знижує рівень часової невизначеності та структурної прихованості сигналу.

На рис. 3.7 наведено процес кореляційного приймання шумоподібних сигналів, сформованих на основі таймерних сигналів (ТСК-6, ТСК-14, ТСК-9) стороннім спостерігачем за умови, що вирішена проблема тактової та циклової синхронізації, а також відома опорна послідовність розширення спектра.

На відміну від класичних шумоподібних позиційних сигналів, для яких у приймачі аналізуються результати перемноження прийнятого та опорного сигналів з подальшим інтегруванням, у випадку таймерних сигналів безпосередньо оцінюється напруга на виході корелятора, яка формується внаслідок збігу часової структури. Розглянемо процес кореляційного накопичення імпульсів таймерних конструкцій на інтервалі t_0 , який описується залежністю

$$U_{\text{інт}}(\tau) = \int_0^{t_0} r(t)s(t - \tau) dt, \quad (3.24)$$

де $r(t)$ – прийнятий шумоподібний таймерний сигнал, $s(t)$ – локально сформована опорна таймерна сигнальна конструкція, t_0 – інтервал інтегрування або тривалість сигнального символу. Вихідна напруга інтегратора $U_{\text{інт}}$ є мірою кореляційного збігу між сигналами. прийнятого та опорного сигналів.

За умови синхронізації часових параметрів накопичення енергії приводить до формування кореляційного максимуму U_{max} , тоді як при відсутності відповідності часових інтервалів або при мінусовому значенні кореляції формується мінімум $-U_{\text{min}}$. Для прийняття рішення використовуються порогові рівні $\pm U_{\text{max}}/2$, які визначають область достовірного виявлення сигнальної конструкції.

Рис. 3.7 (а) демонструє процес інтегрування для випадку часткового збігу часової структури таймерного сигналу (ТСК-6) з опорною реалізацією. ТСК-6 має наступні тривалості імпульсів: $t_{c1} = 5\Delta$; $t_{c2} = 4\Delta$; $t_{c3} = 7\Delta$.

У першому та четвертому часових інтервалах t_0 спостерігається стале накопичення позитивної енергії та досягнення верхнього кореляційного порогу. Але потрібно відзначити, що тривалість першого імпульсу $t_{c1} = t_0 + \Delta = 5\Delta$, а для $t_{c3} = t_0 + 2\Delta = 7\Delta$. Це означає, що правильне відновлення першого імпульсу t_{c1} та

третього імпульсу t_{c3} не є можливим. При цьому можна побачити, що у другому та третьому інтервалах t_0 виникають чергування позитивних і негативних складових, що зумовлено неповним часовим збігом окремих непозиційних імпульсів t_{c1} , t_{c2} та t_{c3} .

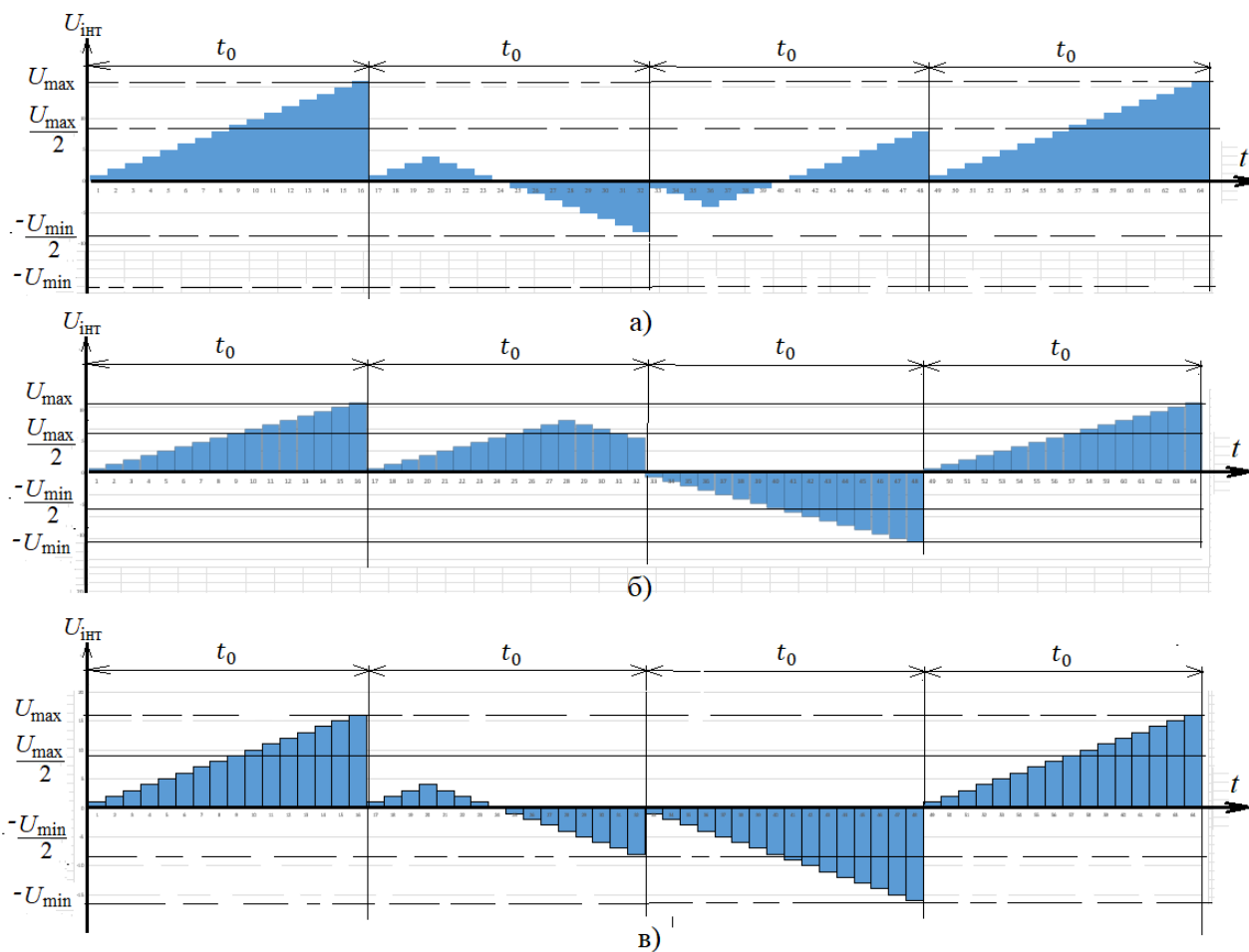


Рис. 3.7. Кореляційне приймання шумоподібного таймерного сигналу

Рис. 3.7 (б) характеризує спроби варіант відновлення структури ТСК-14 ($t_{c1} = 7\Delta$; $t_{c2} = 5\Delta$; $t_{c3} = 4\Delta$), у якому інтегральна напруга змінюється більш плавно, а накопичення енергії відбувається за рахунок послідовного збігу часових положень імпульсів. Позитивна та негативна області мають відносно симетричний характер, що свідчить про зміну ступеня часової відповідності між прийнятою та опорною ТСК.

Рис. 3.7 (в) ілюструє випадок спроби відновлення структури таймерного сигналу ТСК-9 ($t_{c1} = 5\Delta$; $t_{c2} = 7\Delta$; $t_{c3} = 4\Delta$), коли окремі часові ділянки сигналу мають лише частковий кореляційний збіг з опорним сигналом. Унаслідок цього на виході інтегратора формуються локальні позитивні та негативні максимуми меншої амплітуди, які не відображають реальну часову структуру ТСК. На першому інтервалі t_0 відбувається накопичення енергії до рівня, достатнього для прийняття рішення про наявність позитивної посилки. Проте момент прийняття такого рішення вже не відповідає фактичній тривалості першого елемента таймерного сигналу $t_{c1} = 5\Delta$, що свідчить про часове розузгодження між структурою ТСК та позиційним способом кореляційної обробки. На другому інтервалі t_0 напруга на виході інтегратора не досягає порогового рівня прийняття рішення. Це пояснюється тим, що її значення знаходиться поза межами діапазону $-U_{\max 2} \dots + U_{\max 2}$, необхідного для достовірної фіксації інформаційної посилки. Третій і четвертий часові інтервали забезпечують формування відгуку, що відповідає негативним посилкам, однак отримана послідовність не відтворює вихідну структуру таймерного сигналу.

Аналіз залежностей, поданих на рис. 3.7, показує, що форма вихідної напруги інтегратора для таймерних сигналів істотно відрізняється від форми відгуку, характерної для класичних позиційних шумоподібних сигналів. Це пояснюється тим, що у таймерних сигналах ЗММ не мають жорсткої прив'язки до фіксованих часових позицій t_0 , а визначаються структурою міжімпульсних інтервалів. Унаслідок цього класичний кореляційний приймач, орієнтований на позиційні сигнали та фіксований інтервал t_0 , не забезпечує коректного відновлення часової структури ТСК і виділення ЗММ. Отже, процес виділення ЗММ відповідно до виразу (3.21) для непозиційних таймерних сигналів потребує модифікації кореляційної процедури та використання спеціалізованих алгоритмів синхронізації, які враховують змінну тривалість міжімпульсних інтервалів.

У системах ПРС-ПВП або ППРЧ інтегратор накопичує результати перемноження біполярних елементів псевдовипадкової послідовності, а максимуми формуються переважно за рахунок кодового збігу. Для таймерних сигналів

накопичення визначається не лише знаком або кодом, а насамперед часовим положенням непозиційних імпульсів t_c .

Така особливість формує додаткову часову невизначеність та підвищує структурну прихованість сигналу, оскільки для його виявлення або відтворення необхідно знати не тільки псевдовипадкову послідовність, але й часову конфігурацію таймерної сигнальної конструкції, тобто параметри будови m , s та i . Унаслідок цього кореляційне приймання шумоподібних таймерних сигналів забезпечує потенційно вищу прихованість та стійкість до засобів радіоелектронної розвідки порівняно з класичними позиційними методами формування широкосмугових сигналів.

3.4 Алгоритм кореляційного приймання шумоподібних таймерних сигнальних конструкцій на основі аналізу екстремумів інтегральної функції

Одним із основних методів приймання шумоподібних сигналів є кореляційне приймання, яке широко використовується в системах зв'язку з розширенням спектра [44, 56-58]. Класичний алгоритм кореляційного приймання ґрунтується на порівнянні прийнятого сигналу з еталонною сигнальною послідовністю та подальшому інтегруванні результату множення протягом інтервалу символу. Такий підхід є ефективним для позиційних сигнально-кодових конструкцій, у яких інформація визначається фіксованим положенням елементів сигналу у часовій сітці.

Однак для непозиційних таймерних сигналів використання класичного алгоритму кореляційного приймання є практично неможливим [42, 43]. Це пояснюється тим, що інформація в таймерних сигналах визначається не абсолютним положенням імпульсів у межах інтервалу символу t_0 , а часовими відстанями між значущими моментами модуляції t_{ci} . У результаті навіть незначне зміщення моментів переходу сигналу призводить до виникнення часткових кореляційних збігів, що формують декілька локальних максимумів кореляційної функції та ускладнюють процес прийняття рішення.

З метою врахування непозиційної структури таймерних сигналів пропонується модифікований алгоритм кореляційного приймання, в якому рішення про структуру прийнятої сигнальної конструкції приймається не за значенням інтеграла наприкінці інтервалу символу, а за положенням та послідовністю екстремумів вихідної напруги корелятора.

На рис. 3.8 наведено приклад зміни напруги на виході інтегратора під час кореляційного приймання трьох шумоподібних таймерних сигналів. У межах інтервалу формування сигнальної конструкції T_c спостерігається послідовність локальних максимумів $U_{\text{макс}}$ та мінімумів $-U_{\text{макс}}$, які відповідають моментам зміни стану таймерного сигналу.

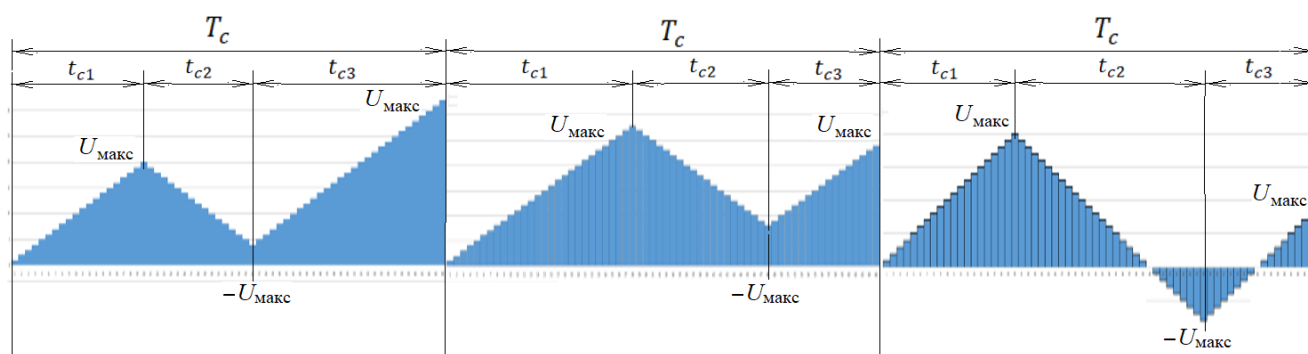


Рисунок 3.8 – Визначення часових інтервалів ТСК за екстремумами вихідної напруги інтегратора в кореляційному приймачі шумоподібних таймерних сигналів

Рішення щодо тривалостей окремих часових інтервалів t_{c1} , t_{c2} та t_{c3} приймається на основі аналізу координат точок екстремумів $U_{\text{макс}}$ та $-U_{\text{макс}}$, які відповідають значущим моментам відновлення (ЗМВ) таймерної сигнальної конструкції. Максимуми кореляційної функції формуються в моменти найбільшого збігу між прийнятим та еталонним сигналами і визначають положення ЗМВ, що характеризують межі інформаційних часових інтервалів. Мінімуми кореляційної функції відображають зміну полярності або структури окремих ділянок сигналу та також можуть використовуватися як додаткові орієнтири для локалізації ЗМВ. Визначення послідовності ЗМВ дозволяє реконструювати часову структуру

таймерного сигналу, встановити тривалості інформаційних інтервалів та відновити передану сигнально-кодову конструкцію.

На відміну від класичного позиційного приймання [33, 34, 41], запропонований підхід орієнтований на аналіз часового розташування екстремумів кореляційної функції, що забезпечує коректне відновлення ЗМВ непозиційних сигнально-кодових конструкцій навіть за наявності значної структурної невизначеності сигналу. Використання такого алгоритму дозволяє реалізувати кореляційне приймання шумоподібних таймерних сигналів із збереженням їх переваг щодо структурної прихованості та завадостійкості.

Отже, запропонований алгоритм кореляційного приймання враховує непозиційну структуру таймерних конструкцій та базується на аналізі положення екстремумів вихідної напруги інтегратора. Це дозволяє відновлювати часову структуру таймерних сигналів за значеннями $U_{\text{макс}}$ та $-U_{\text{макс}}$ у межах інтервалу T_c , що забезпечує коректне приймання шумоподібних таймерних сигналів і підвищує ефективність їх використання в системах прихованого радіозв'язку.

3.5 Оцінка ефективності методів захисту інформації на основі широкосмугових сигналів

Ефективність методів захисту інформації в системах радіозв'язку визначається їх здатністю забезпечувати одночасно прихованість передавання, завадостійкість та раціональне використання енергетичних і спектральних ресурсів. Для сучасних систем військового зв'язку ці вимоги є взаємопов'язаними, оскільки підвищення одного показника часто супроводжується погіршенням іншого [38,43]. Наприклад, збільшення швидкості передавання може знижувати енергетичну прихованість, тоді як надмірне розширення спектра здатне підвищувати енергетичні витрати системи. Тому оцінювання ефективності методів захисту інформації повинно базуватись на комплексному аналізі їхніх характеристик.

Критерії оцінки ефективності методів розширення спектра формуються з урахуванням особливостей функціонування систем зв'язку в умовах радіоелектронної протидії. До основних критеріїв належать:

- енергетична прихованість;
- структурна прихованість;
- завадостійкість;
- спектральна ефективність;
- енергетична ефективність;
- криптографічна стійкість;
- складність реалізації.

Першочерговим критерієм для систем прихованого зв'язку є енергетична прихованість, яка характеризує здатність сигналу залишатися малопомітним для засобів радіоелектронної розвідки. Імовірність виявлення сигналу енергетичним детектором визначається через співвідношення сигнал/шум та порогове правило прийняття рішення [34]:

$$P_{\text{вияв}} = P(Y > \lambda \mid H_1), \quad (3.25)$$

де Y – статистика детектора; λ – поріг виявлення; H_1 – гіпотеза про наявність сигналу. Для енергетичного детектора статистика має вигляд

$$Y = \sum_{n=1}^N |r(n)|^2, \quad (3.26)$$

де $r(n)$ – прийнятий сигнал; N – кількість відліків. При цьому прийнятий сигнал описується системою гіпотез:

$$\begin{cases} H_0: r(n) = w(n), \\ H_1: r(n) = s(n) + w(n), \end{cases} \quad (3.27)$$

де $w(n)$ – шум; $s(n)$ – корисний сигнал. Зниження спектральної густини потужності

$$S(f) = \lim_{T \rightarrow \infty} \frac{|X_T(f)|^2}{T} \quad (3.28)$$

призводить до зменшення ймовірності виявлення, що підвищує енергетичну прихованість системи.

Другим важливим критерієм є структурна прихованість, яка визначає складність розпізнавання структури сигналу після його виявлення. Для сигналів із розширеним спектром структурна прихованість залежить від ансамблю можливих сигнально-кодових конструкцій [38, 44, 47, 50]:

$$S_{\text{стр}} = \log_2 L, \quad (3.29)$$

де L – число можливих реалізацій сигналу.

Для ППРЧ-систем

$$L_{\text{ППРЧ}} = M^L, \quad (3.30)$$

де M – кількість частотних позицій; L – довжина псевдовипадкової послідовності.

Для таймерних сигналів загальну кількість реалізацій ТСК можна визначити за формулою (3.9), що забезпечує додатковий рівень структурної невизначеності.

Показником завадостійкості є ймовірність бітової помилки, яка визначає достовірність передавання інформації. Для двійкової фазової маніпуляції у каналі з адитивним білим гаусівським шумом [19]:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \quad (3.31)$$

де $Q(\cdot)$ – інтеграл імовірності; E_b/N_0 – енергетична ефективність. У системах із розширеним спектром завадостійкість додатково визначається коефіцієнтом розширення:

$$G_p = \frac{B_s}{R}, \quad (3.32)$$

де B_s – ширина спектра сигналу; R – швидкість передавання. Чим більший коефіцієнт обробного виграшу G_p , тим вища стійкість до вузькосмугових завад та навмисного радіоподавлення.

Оцінка спектральної ефективності є необхідною для визначення раціональності використання частотного ресурсу. Спектральна ефективність визначається як

$$\eta_f = \frac{R}{B}, \quad (3.33)$$

де R – швидкість передавання; B – смуга частот.

Методи розширення спектра, як правило, характеризуються нижчою спектральною ефективністю порівняно з вузькосмуговими системами, однак забезпечують вищу прихованість та завадостійкість. Енергетична ефективність оцінюється через відношення енергії біта до спектральної густини шуму:

$$\eta_e = \frac{E_b}{N_0}. \quad (3.34)$$

Між спектральною та енергетичною ефективністю існує фундаментальний компроміс, описаний співвідношенням

$$\frac{E_b}{N_0} = \frac{2^{\eta_f} - 1}{\eta_f}, \quad (3.35)$$

яке впливає з теореми пропускної здатності каналу.

Для комплексної оцінки методів захисту інформації доцільно використовувати інтегральний критерій ефективності:

$$K_{\text{еф}} = w_1 K_{\text{пр}} + w_2 K_3 + w_3 K_{\text{е}} + w_4 K_{\text{с}}, \quad (3.36)$$

де $K_{\text{пр}}$ – показник прихованості; K_3 – завадостійкість; $K_{\text{е}}$ – енергоефективність; $K_{\text{с}}$ – спектральна ефективність; w_i – вагові коефіцієнти. Такий метод оцінки дозволяє враховувати специфіку конкретної системи зв'язку та її пріоритети.

Порівняльний аналіз методів розширення спектра свідчить про наявність суттєвих відмінностей у їхніх характеристиках. Системи з ПРС-ПВП забезпечують високий обробний виграш і добру стійкість до вузькосмугових завад, проте мають обмежену структурну прихованість через можливість кореляційного виявлення псевдовипадкових послідовностей. Системи з ППРЧ характеризуються високою стійкістю до прицільного радіоподавлення та кращою частотною адаптивністю, однак можуть бути вразливими до аналізу частотних закономірностей при компрометації керуючих послідовностей.

Комбінований метод на основі ПРС-ПВП–ППРЧ частково усувають ці недоліки, забезпечуючи одночасно кодове та частотне розширення спектра, але ціною значного ускладнення апаратної реалізації та синхронізації.

Таймерні сигнали мають додаткову перевагу, пов'язану з формуванням часової невизначеності. У цьому випадку структурна прихованість визначається не лише частотними або кодовими параметрами, а й часовою структурою сигналу. Комбінування ТСК з ППРЧ формує багатовимірний простір невизначеності, який може бути оцінений як

$$L_{\text{comb}} = L_{\text{ТСК}} \cdot M^L. \quad (3.37)$$

Зростання числа можливих реалізацій суттєво ускладнює структурне виявлення та перехоплення інформації. Отже, оцінювання ефективності методів

захисту інформації повинно базуватися на комплексному врахуванні прихованості, завадостійкості, спектральної та енергетичної ефективності. Проведений аналіз показує, що класичні методи ПРС-ПВП та ППРЧ забезпечують високий рівень захисту, однак мають обмеження щодо структурної прихованості. Перспективним напрямом подальшого розвитку є інтеграція методів розширення спектра з таймерними сигналами, що створює передумови для формування нових систем прихованого та завадозахищеного радіозв'язку.

3.6 Висновки до розділу 3

1. Проведено дослідження принципів побудови позиційних і непозиційних сигналів та встановлено, що таймерні сигнальні конструкції належать до класу непозиційних сигналів, у яких інформація визначається сукупністю часових інтервалів між значущими моментами модуляції. Такий підхід забезпечує додатковий часовий ступінь свободи під час кодування інформації та створює передумови для підвищення структурної прихованості сигналів.

2. Розроблено математичні моделі таймерних сигнальних конструкцій та досліджено закономірності їх формування. Показано, що кількість можливих реалізацій ТСК визначається параметрами m , ста i зростає за комбінаторним законом. Встановлено, що збільшення параметрів побудови призводить до суттєвого розширення ансамблю сигнально-кодових конструкцій порівняно з класичними позиційними кодами.

3. Виконано аналіз спектральних властивостей таймерних сигналів. Встановлено, що нерегулярний розподіл значущих моментів модуляції формує шумоподібний спектр із менш вираженими дискретними складовими, що сприяє зменшенню ймовірності спектрального виявлення та підвищує енергетичну прихованість сигналів.

4. Проведено дослідження кореляційних властивостей ансамблю таймерних сигнальних конструкцій. Встановлено залежність між коефіцієнтами взаємної кореляції та кодовою відстанню між сигналами: зі збільшенням кодової відстані

спостерігається зниження рівня взаємної кореляції. Для досліджуваного ансамблю із 15 таймерних сигналів визначено середній коефіцієнт взаємної кореляції $\bar{r} \approx 0,64$, а коефіцієнт ортогональності становив $K_{\text{орт}} = 0,36$, що підтверджує наявність слабокорельованих сигнальних конструкцій та можливість формування шумоподібних сигналів із підвищеною структурною прихованістю.

5. Досліджено процес кореляційного приймання таймерних сигналів та показано, що класичні алгоритми приймання, орієнтовані на позиційні сигнали з фіксованою часовою структурою, не забезпечують коректного відновлення ТСК. Запропоновано підхід до приймання, заснований на визначенні значущих моментів відновлення за координатами екстремумів вихідної напруги кореляційного інтегратора, що дозволяє відновлювати часову структуру таймерного сигналу та визначати його інформаційні параметри.

6. Отримані результати підтвердили, що використання таймерних сигнальних конструкцій забезпечує додаткову часову невизначеність, знижує рівень статистичної передбачуваності сигналів та підвищує їх структурну прихованість ще до застосування методів розширення спектра. Це створює теоретичне підґрунтя для подальшої інтеграції ТСК з технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот з метою формування комбінованих шумоподібних сигналів для захищених систем радіозв'язку.

РОЗДІЛ 4

РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕТОДІВ РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ

У четвертому розділі дисертаційної роботи досліджено та розроблено методи формування шумоподібних таймерних сигналів на основі процедур розширення спектра. Проведено аналіз параметрів таймерних сигнальних конструкцій та їх відмінностей від позиційних сигналів, визначено вплив параметрів m , s та i на кількість можливих реалізацій і рівень структурної прихованості. Виконано порівняльне оцінювання спектральної та енергетичної ефективності позиційних і таймерних сигналів, що підтвердило доцільність використання ТСК як основи шумоподібних сигнальних конструкцій. Розроблено методи розширення спектра таймерних сигналів на основі прямого розширення спектра та псевдовипадкового перескоку робочих частот, зокрема швидкого, повільного та багатоканального режимів ППРЧ. Запропоновано математичні моделі та алгоритми формування комбінованих сигналів у просторі «час–код–частота». Проведено оцінювання структурної прихованості та інтегральної бази сигналу, а також досліджено вплив параметрів ТСК, ПВП і ППРЧ на рівень невизначеності сигнальної структури. Отримані результати підтвердили можливість суттєвого підвищення структурної прихованості та шумоподібності сигналів шляхом комбінованого використання таймерного кодування і методів розширення спектра.

4.1 Аналіз параметрів таймерних сигнальних конструкцій для реалізації маніпуляції та розширення спектра

Позиційні сигнали, як правило, використовуються у системах цифрового зв'язку та лежать в основі більшості класичних методів модуляції і розширення спектра [35, 41, 43, 61, 62]. Їх характерною особливістю є передавання інформації за рахунок фіксованого розташування інформаційних елементів у часі або частоті.

При цьому кожному біту відповідає визначена позиція імпульсу в межах тактового інтервалу t_0 . При такому способі представлення імпульсів забезпечує відносну простоту синхронізації, маніпуляції та декодування, однак обмежує кількість можливих сигнальних реалізацій та формує передбачувану часову структуру сигналу [33, 34], що спрощує його виявлення і структурний аналіз засобами радіоелектронної розвідки.

На відміну від позиційного кодування, таймерні сигнали реалізують непозиційний принцип формування часової структури імпульсів в межах комбінації T_c [46-49]. При цьому ЗММ визначається не абсолютним положенням імпульсу, а тривалістю міжімпульсних інтервалів t_{ci} у межах сигнальної конструкції. У цьому випадку сигнальний стан формується сукупністю часових інтервалів між ЗММ, що забезпечує суттєве ускладнення часової структури сигналу та підвищує рівень його структурної прихованості. Формування ТСК здійснюється на інтервалі

$$T_c = mt_0, \quad (4.1)$$

де t_0 – базовий інтервал Найквіста, а m – кількість таких інтервалів у межах сигнальної конструкції. Параметр m визначає часову довжину ТСК T_c та безпосередньо впливає на число можливих сигнальних реалізацій. Модель формування міжімпульсних інтервалів ТСК визначається виразом

$$t_c = t_0 + k\Delta, \quad (4.2)$$

де k – індекс варіювання тривалості інтервалу, а

$$\Delta = \frac{t_0}{s} \quad (4.3)$$

– дробовий часовий елемент формування сигналу. Параметр s характеризує рівень часової дискретизації та визначає, у скільки разів елемент Δ менший за базовий інтервал t_0 . Використання дробового кроку Δ дозволяє формувати значну кількість різних міжімпульсних структур у межах одного інтервалу T_c , що є принциповою відмінністю ТСК від класичних позиційних кодів.

Третім важливим параметром є i , який визначає кількість ЗММ у межах сигнальної конструкції. Параметр i характеризує число інформаційних інтервалів, які використовуються при формуванні ТСК. Зі збільшенням i ускладняється часова структура комбінації та зростає число його можливих реалізацій.

Кількість різних реалізацій таймерних сигнальних конструкцій на інтервалі T_c визначається комбінаторним співвідношенням [19]

$$N_{\text{тск}} = \frac{[ms-(s-1)i]!}{i!([ms-(s-1)i]-i)!} \quad (4.4)$$

де N_p – кількість можливих ТСК. Залежність N_p від параметрів m , s та i має експоненційний характер.

З табл. 4.1 – 4.3 можна побачити, що збільшення параметра m приводить до розширення часового інтервалу формування ТСК, яке забезпечує зростання кількості можливих комбінацій. Наприклад, для параметрів $m = 4$, $s = 4$ та $i = 2$ отримуємо $N_{\text{тск}} = 45$. Для $m = 9$, $s = 4$ та $i = 2$ кількість реалізацій значно збільшується $N_{\text{тск}} = 435$.

Аналогічно, підвищення параметра s зменшує величину дробового інтервалу Δ , збільшуючи число допустимих варіантів побудови міжімпульсних інтервалів. Наприклад, для параметрів $m = 5$, $s = 4$ та $i = 2$ кількість реалізацій $N_{\text{тск}} = 91$. Для $m = 5$, $s = 6$ та $i = 2$ кількість реалізацій збільшилося $N_{\text{тск}} = 190$. В цьому прикладі можна побачити, що кількість реалізацій ТСК збільшується без розширення інтервалу часу побудови комбінації T_c . Проте це досягається за рахунок зменшення базового інтервалу побудови ТСК Δ , а також падіння завадостійкості в системі зв'язку.

Варіювання параметром i також суттєво впливає на число сигнальних станів, оскільки змінює кількість інформаційних елементів у структурі ТСК. Характерним при цьому є той факт, що збільшення кількості ЗММ може як збільшити число реалізацій, так і зменшити. З табл. 4.1 – 4.3 наведемо приклад зменшення числа реалізацій. Наприклад, для параметрів побудови ТСК $m = 4$, $s = 4$ та $i = 2$ отримуємо $N_{\text{ТСК}} = 45$. Проте при $i = 3$ кількість реалізацій зменшується та становить $N_{\text{ТСК}} = 35$ (табл. 4.2). З табл. 4.3 можна побачити, що для $i = 4$, $m = 4$ та $s = 4$ взагалі не можливо побудови ТСК з таким числом ЗММ.

Таблиця 4.1

Кількість таймерних сигналів в залежності від m , s та $i=2$

m	s	$i=2$				Сума
		3	4	5	6	
4		28	45	66	91	245
5		55	91	136	190	500
6		91	153	231	325	845
7		136	231	351	496	1280
8		190	325	496	703	1805
9		253	435	666	946	2420

Таблиця 4.2

Кількість таймерних сигналів в залежності від m , s та $i=3$

m	s	$i=3$				Сума
		3	4	5	6	
4		20	35	56	84	205
5		84	165	286	455	1025
6		220	455	816	1330	2905
7		455	969	1771	2925	6285
8		816	1771	3276	5456	11605
9		1330	2925	5456	9139	19305

Збільшення числа реалізацій N_p безпосередньо впливає на структурну прихованість сигналу. Структурна прихованість характеризує невизначеність сигнальної конструкції для стороннього спостерігача та може бути оцінена як [52, 57, 66, 67]

$$S_{\text{стр}} = \log_2 N_p. \quad (4.5)$$

Таблиця 4.3

Кількість таймерних сигналів в залежності від m , s та $i=3$

m	s	$i=4$				Сума
		3	4	5	6	
4		-	-	-	-	-
5		35	70	126	210	456
6		210	495	1001	1820	3596
7		715	1820	3876	7315	13936
8		1820	4845	10626	20475	38261
9		3876	10626	23751	46376	85630

Із формули (4.5) можна зробити висновок, що зростання кількості реалізацій ТСК призводить до підвищення рівня структурної прихованості. Для потенційного порушника це означає необхідність аналізу значно більшої множини можливих сигнальних структур, що ускладнює виявлення та декодування повідомлення без знання параметрів формування ТСК.

Разом із тим збільшення параметрів m та s породжує певне протиріччя між прихованістю та завадостійкістю. Зменшення інтервалу Δ підвищує структурну різноманітність сигналів, але одночасно зменшує енергетичну відстань між сусідніми сигнальними реалізаціями. У результаті зростають вимоги до точності тактової та циклової синхронізації, а також ускладнюються процеси генерації та декодування ТСК.

Особливий інтерес ТСК становлять з точки зору реалізації процедур маніпуляції [59] та подальшого розширення спектра. На відміну від позиційних

сигналів, де маніпуляція здійснюється за рахунок зміни параметрів імпульсів фіксованого тактового інтервалу t_0 , у ТСК маніпуляція пов'язана з варіюванням часових параметрів міжімпульсних інтервалів. Це принципово змінює підхід до формування модульованих сигналів.

Загальна кількість можливих станів маніпуляції визначається співвідношенням

$$N_M = 2^{k_\Delta}, \quad (4.6)$$

де k_Δ – кількість часових інтервалів Δ , що використовуються для реалізації конкретного виду маніпуляції.

Наприклад, для двійкової фазової маніпуляції (BPSK) достатньо одного інтервалу Δ , тоді як квадратурна фазова маніпуляція (QPSK) потребує використання двох часових станів. Для багаторівневих схем, зокрема QAM, число необхідних інтервалів Δ зростає. Це створює можливість реалізації багатовимірної часово-фазової структури сигналу.

Отже, таймерні сигнали характеризуються суттєво більшою варіативністю сигнальних реалізацій порівняно з позиційними кодами. Використання параметрів m , s та i забезпечує цілеспрямоване керування структурною прихованістю, а непозиційний принцип кодування створює передумови для реалізації нових методів маніпуляції та подальшого розширення спектра в часовій і частотній областях. Це обґрунтовує доцільність застосування ТСК як основи для формування шумоподібних сигналів із підвищеним рівнем прихованості передавання інформації.

4.2 Порівняльний аналіз спектральної та енергетичної ефективності позиційних і таймерних сигналів

Ефективність використання частотного та енергетичного ресурсу є одним із ключових критеріїв оцінювання сучасних систем захищеного радіозв'язку. У

системах передавання інформації ці показники визначають можливість забезпечення необхідної швидкості передавання даних, рівня завадостійкості та прихованості сигналу. Для обґрунтування доцільності використання ТСК при синтезі шумоподібних сигналів необхідно здійснити їх порівняння з позиційними сигналами за показниками спектральної та енергетичної ефективності.

Спектральна ефективність характеризує ступінь використання смуги частот каналу зв'язку та визначається як відношення швидкості передавання інформації до займаної смуги частот [19]:

$$\gamma = \frac{R}{\Delta F}, \quad (4.7)$$

де R – швидкість передавання інформації, біт/с; ΔF – ширина спектра сигналу, Гц.

З (4.7) випливає, що збільшення спектральної ефективності означає можливість передавання більшого обсягу інформації у заданій смузі частот. Для систем захищеного зв'язку цей показник є особливо важливим, оскільки розширення спектра повинно поєднуватися з раціональним використанням частотного ресурсу.

Для класичних позиційних сигналів ширина спектра визначається тривалістю елементарного тактового інтервалу t_0 . За умови використання імпульсів прямокутної форми оцінка смуги частот має вигляд

$$\Delta F_{\text{ПК}} = \frac{1}{t_0}. \quad (4.8)$$

Це означає, що спектральні характеристики позиційного сигналу визначаються фіксованою тривалістю інформаційного елемента. Зменшення t_0 приводить до розширення спектра та підвищення швидкості передавання, однак одночасно зростають вимоги до синхронізації та енергетичних характеристик каналу.

На відміну від позиційних кодів, у ТСК тривалість міжімпульсних інтервалів є змінною та формується відповідно до співвідношення $t_c = t_0 + k\Delta$. Тому спектральні характеристики ТСК визначаються не лише базовим інтервалом t_0 , а й параметрами таймерного кодування k та s . Для таких сигналів оцінка ширини спектра може бути представлена як

$$\Delta F_{\text{ТСК}} \leq \frac{1}{t_c} = \frac{1}{t_0 + k\Delta}. \quad (4.9)$$

Вираз (4.9) свідчить, що смуга частот ТСК має змінну складову та залежить від структури часових інтервалів. При цьому розширення сигнального простору здійснюється не лише за рахунок зміни частотної області, а й шляхом варіювання часової структури сигналу. Спектральна ефективність ТСК відповідно до (4.7) визначається як

$$\gamma_{\text{ТСК}} = \frac{R}{\Delta F_{\text{ТСК}}}. \quad (4.10)$$

За однакових умов використання смуги частот $\Delta F_{\text{ТСК}} = \Delta F_{\text{ПК}}$ виконується співвідношення

$$\gamma_{\text{ТСК}} \geq \gamma_{\text{ПК}}. \quad (4.11)$$

Отриманий результат пояснюється тим, що у ТСК інформація кодується не фіксованими часовими позиціями, а структурою міжімпульсних інтервалів. Це дозволяє збільшити кількість можливих сигнальних реалізацій без пропорційного збільшення смуги частот. Фактично розширення сигнального простору відбувається в часовій області, що забезпечує ефективніше використання спектрального ресурсу.

Поряд із спектральною ефективністю важливим показником є енергетична ефективність сигналу, яка визначається співвідношенням енергії біта до спектральної густини шуму [33, 34]:

$$\beta = \frac{E_b}{N_0}, \quad (4.12)$$

де E_b – енергія біта; N_0 – спектральна густина потужності шуму.

Показник β характеризує мінімальні енергетичні витрати, необхідні для забезпечення заданої достовірності прийому. Для позиційних сигналів підвищення спектральної ефективності зазвичай супроводжується зростанням вимог до енергетичного ресурсу каналу. Це пояснюється тим, що зменшення тривалості інформаційних імпульсів та збільшення швидкості передавання знижує енергетичну відстань між сигнальними станами.

У ТСК аналогічне протиріччя також присутнє, проте воно проявляється інакше. Збільшення параметра s зменшує часовий інтервал $\Delta = t_0/s$, що дозволяє формувати більшу кількість сигнальних конструкцій та підвищувати структурну прихованість. Однак одночасно зменшується енергетична відстань між сусідніми ТСК, що може призводити до погіршення завадостійкості та потребує точнішої синхронізації. Попри зазначене протиріччя, ТСК мають низку переваг при формуванні шумоподібних сигналів. Передусім змінна структура міжімпульсних інтервалів забезпечує:

- формування багатовимірної часово-частотної структури сигналу;
- підвищення ентропії та шумоподібності сигнальної конструкції;
- зростання структурної прихованості;
- ускладнення процесів виявлення та класифікації сигналу;
- можливість реалізації розширення спектра без суттєвого збільшення смуги частот.

На відміну від класичних позиційних сигналів, де шумоподібність формується переважно за рахунок псевдовипадкових кодів або перебудови частоти,

ТСК забезпечують додатковий рівень невизначеності завдяки неперіодичній часовій структурі. Це створює передумови для формування сигналів із підвищеною структурною прихованістю та ускладнює їх аналіз засобами радіоелектронної розвідки.

Отже, результати порівняльного аналізу свідчать, що таймерні сигнальні конструкції забезпечують ефективніше використання спектрального ресурсу порівняно з позиційними кодами та створюють додаткові можливості для підвищення структурної прихованості сигналу. Незважаючи на певне зниження енергетичної відстані між сигнальними реалізаціями при великих значеннях параметра s , використання ТСК є доцільним для побудови шумоподібних сигналів із комбінованим розширенням спектра, оскільки дозволяє реалізувати розширення сигнального простору одночасно в часовій і частотній областях.

4.3 Розробка методів розширення спектра таймерних сигналів на основі псевдовипадкового перескоку робочих частот

4.3.1 Аналіз методів ППРЧ для позиційних сигналів

Обґрунтованість застосування шумоподібних таймерних сигналів пояснюється необхідністю ускладнення структури сигнальних конструкцій для підвищення структурної та енергетичної прихованості передавання інформації. Особливість таймерних сигнальних конструкцій полягає в тому, що вони належать до класу непозиційних сигналів, у яких інформація визначається не фіксованими часовими позиціями імпульсів, а тривалістю міжімпульсних інтервалів. Такий принцип побудови забезпечує низку переваг порівняно з позиційними сигналами, зокрема можливість формування великої кількості сигнальних реалізацій, реалізації завадостійкого кодування без використання додаткових перевірочних елементів та підвищення структурної прихованості сигналу.

Зміна параметрів пристрою кодування ТСК дозволяє формувати різні ансамблі сигнальних конструкцій із заданими статистичними та кореляційними

властивостями. Це створює передумови для використання таймерних сигналів у широкосмугових системах зв'язку та інтеграції їх із методами розширення спектра.

Для розроблення методу розширення спектра таймерних сигналів на основі ППРЧ спочатку проаналізуємо класичні методи [22-26], що застосовуються для позиційних сигналів. Відомі методи ППРЧ орієнтовані переважно на позиційні коди, у яких ЗММ визначаються з урахуванням фіксованого інтервалу часу елементарної послідовності t_0 . Залежно від співвідношення між тривалістю роботи на одній частоті та тривалістю символу t_0 розрізняють швидку, повільну та багатоканальну ППРЧ. Кожен із зазначених методів має власні переваги та обмеження, що визначають їх придатність до конкретних умов застосування.

У класичному методі швидкої ППРЧ зміна робочої частоти відбувається швидше, ніж передавання одного інформаційного символу, тобто протягом інтервалу t_0 частота несучої може змінюватися декілька разів. Такий режим формально описується умовою

$$T_f \leq t_0, \quad (4.13)$$

де T_f – тривалість передавання сигналу на одній робочій частоті.

За такого режиму один інформаційний символ або його окремі фрагменти передаються на декількох робочих частотах, вибір яких здійснюється відповідно до псевдовипадкового закону. Це забезпечує високу стійкість до вузькосмугових і навмисних завад, оскільки вплив перешкоди обмежується лише частиною спектрально-часової структури сигналу. Крім того, швидкий перескок робочої частоти підвищує енергетичну прихованість, оскільки без знання алгоритму зміни частот ускладнюється процес виявлення та супроводження сигналу засобами радіоелектронної розвідки. Разом із тим швидка ППРЧ висуває підвищені вимоги до синхронізації передавача і приймача, а також до швидкодії апаратури формування та перебудови несучих частот. Це збільшує складність технічної реалізації та енергетичні витрати системи.

Для методу повільної ППРЧ зміна робочої частоти відбувається повільніше, ніж тривалість передавання одного інформаційного символу, тобто на одній частоті передається декілька інформаційних символів. Цей метод формально характеризується умовою:

$$T_f > t_0, \quad (4.14)$$

Цей метод має простішу реалізацію порівняно зі швидкою ППРЧ, оскільки зміна частоти відбувається рідше, і менші вимоги до синхронізації, що робить його більш придатним для систем з обмеженими ресурсами. Проте він має нижчу енергетичну прихованість, оскільки сигнал довше знаходиться на одній частоті, що полегшує його виявлення, а також низьку стійкість до вузькосмугових завад.

У методі багатоканальної ППРЧ кожен інформаційний символ передається одночасно на декількох частотах, що дозволяє підвищити стійкість системи до завад завдяки дублюванню інформації. Для кожного символу вибирається набір частот $\{f_{i1}, f_{i2}, \dots, f_{iw}\}$, де w – кількість підканалів.

В залежності від методу ППРЧ інтервал розширення T_f впливає на кількість елементів $M_{\text{швид ППРЧ}}$, які передаються на одній частоті з тривалістю t_0 . Для швидкої ППРЧ $T_f \leq t_0$, тому на одній частоті передається тільки частина одного біту. Кількість робочих частот на інтервалі t_0 для швидкої ППРЧ визначається як:

$$M_{\text{швид ППРЧ}} = \left\lfloor \frac{t_0}{T_f} \right\rfloor, \quad (4.15)$$

Для повільної ППРЧ $T_f > t_0$, тому на одній частоті передається декілька символів, і кількість елементів m визначається як:

$$M_{\text{пов ППРЧ}} = \left\lfloor \frac{T_f}{t_0} \right\rfloor, \quad (4.16)$$

де $\lfloor \cdot \rfloor$ – операція взяття цілої частини. Наприклад, якщо $T_f = 3t_0$, то $m = 3$, тобто на одній частоті передається 3 інформаційних символи.

Для багатоканальної ППРЧ кожен інформаційний символ або група символів передається одночасно на декількох робочих частотах, що забезпечує частотне рознесення та підвищує завадостійкість системи. Для передавання використовується множина частот

$$F_i = \{f_{i1}, f_{i2}, \dots, f_{iw}\}, \quad (4.17)$$

де w – кількість паралельних частотних підканалів.

Незважаючи на переваги методів ППРЧ для позиційних кодів, їхнє застосування для непозиційних сигналів, таких як таймерні сигнали, ускладнене через відсутність фіксованої прив'язки значущих моментів модуляції до часових інтервалів t_0 . У таймерних сигналах ЗММ не прив'язані до інтервалу Найквіста t_0 , а їхня тривалість може змінюватися в межах. Тривалість імпульсів таймерних сигналів $= t_c = t_0 + \Delta k$ може змінювати на певну кількість Δ в межах комбінації. Це робить класичні методи ППРЧ, орієнтовані на позиційні коди, непридатними для таймерних сигналів без додаткових модифікацій. Отже, для застосування ППРЧ у системах з непозиційними сигналами потрібно розробити відповідні алгоритми, які враховують особливості формування і передавання таких сигналів.

4.3.2 Метод швидкого ППРЧ для розширення спектра таймерних сигналів

У методі швидкої ППРЧ для позиційних кодів зміна робочої частоти відбувається швидше, ніж тривалість передавання одного інформаційного символу, тобто $T_f \leq t_0$. Проте на відміну від позиційних сигналів [27, 28], для таймерних сигналів принцип швидкої ППРЧ потребує додаткового врахування непозиційної часової структури. ЗММ у ТСК визначаються варіаціями міжімпульсних інтервалів $t_c = t_0 + k\Delta$. Непозиційність таймерної конструкції робить доцільним перескок

робочої частоти не відносно інтервалу t_0 , а в межах одного або декількох інтервалів Δ . В цьому випадку швидка ППРЧ для ТСК описується умовою [37]:

$$T_f \leq M_{\text{швид ППРЧ-ТСК}} \times \Delta, \quad (4.18)$$

де T_f – інтервал перебування сигналу на одній робочій частоті; $M_{\text{швид ППРЧ-ТСК}} = 1, 2, \dots$ – кількість елементарних часових інтервалів Δ , протягом яких зберігається поточна частота.

Визначимо два режими роботи швидкої ППРЧ для ТСК. При $M_{\text{швид ППРЧ-ТСК}} = 1$ реалізується максимальна швидкість перескоку, коли зміна частоти відбувається після кожного елементарного інтервалу Δ . У цьому випадку кожний фрагмент таймерної структури передається на окремій робочій частоті, що забезпечує найвищий рівень енергетичної та структурної прихованості сигналу. При $M_{\text{швид ППРЧ-ТСК}} > 1$ одна й та сама частота використовується для передавання декількох інтервалів Δ .

Для опису сигналу, сформованого за допомогою швидкої ППРЧ для ТСК, можна використати наступну модель модуляції. Таймерний сигнал $S_{\text{ТСК}}(t)$ формується як послідовність імпульсів, де кожен імпульс має тривалість $t_c = t_0 + k\Delta$, але модуляція та розширення спектра здійснюються відносно інтервалу Δ . Таким чином, сигнал може бути представлений у вигляді:

$$S_{\text{ТСК}}(t) = \sum_{n=0}^{N-1} A \cdot p(t - n \cdot \Delta), \quad (4.19)$$

де A – амплітуда імпульсу; $p(*)$ – імпульсна характеристика; N – кількість імпульсів у сигналі, виражена в інтервалах Δ .

Сигнал $S_{\text{ТСК}}(t)$ модулюється за допомогою псевдовипадкового перескоку частоти, де несуча частота f_c змінюється на кожному інтервалі Δ згідно з законом:

$$f_c(n\Delta) = f_0 + \Delta f \cdot c(n), \quad (4.20)$$

де f_0 – базова частота, Δf – крок зміни частоти, $c(n)$ – псевдовипадкова послідовність, яка визначає закон зміни частоти на кожному інтервалі Δ .

Модульований сигнал може бути записаний як:

$$S_{\text{ППРЧ}}(t) = \sum_{n=0}^{N-1} A \cdot p(t - n\Delta) \cdot \cos \left(2\pi \int_0^t f_c(\tau) d\tau \right). \quad (4.21)$$

Спектр сигналу $S_{\text{ППРЧ}}(t)$ визначається суперпозицією спектрів окремих імпульсів, зсунутих за частотою згідно з законом $f_c(n\Delta)$. Ширина спектра сигналу залежить від: тривалості імпульсів Δ ; кроку зміни частоти Δf ; швидкості перескоку частоти, яка визначається параметром $M_{\text{швид}} \text{ ППРЧ-ТСК}$.

Таким чином, усі процеси модуляції та розширення спектра узгоджені з елементарним інтервалом Δ , що є основою для формування таймерних сигналів.

4.3.3 Метод повільного ППРЧ для розширення спектра таймерних сигналів

Для позиційних сигналів метод повільної ППРЧ реалізується шляхом передавання декількох інформаційних символів на незмінній несучій частоті, коли інтервал перебування на одній частоті перевищує тривалість інформаційного символу, тобто $T_f > t_0$ [37]. Цей підхід забезпечує простішу реалізацію передавача та приймача, а також зменшує вимоги до швидкодії систем синхронізації.

На відміну від швидкої ППРЧ, у якій перебудова частоти виконується в межах одного або декількох інтервалів Δ , метод повільної ППРЧ для таймерних сигналів передбачає передавання однієї або декількох груп елементів Δ на одній робочій частоті. З урахуванням змінної тривалості інтервалів ТСК умову повільної ППРЧ доцільно формулювати не відносно t_0 , а відносно інтервалів таймерного сигналу Δ . Тоді інтервал перебування на одній частоті повинен перевищувати тривалість однієї групи елементів Δ , тобто:

$$T_f > L \cdot \Delta, \quad (4.22)$$

де $L \geq 1$ – кількість елементів Δ у одній групі. Це означає, що одна робоча частота використовується для передавання однієї або декількох груп елементів Δ без зміни несучої. Кількість таймерних елементів, що передаються на одній частоті, визначається як:

$$M_{\text{пов ППРЧ-ТСК}} = \left\lfloor \frac{T_f}{\Delta} \right\rfloor = K \cdot L, \quad (4.23)$$

де K – кількість груп елементів Δ , що передаються на одній частоті; $L \geq 1$ – кількість елементів Δ у одній групі. Наприклад, якщо $T_f = 8\Delta$, $L = 2$, то $K = 4$, і на одній частоті передаються чотири групи по два імпульсні елементи тривалістю Δ .

Нехай множина доступних робочих частот визначається як:

$$F = \{f_1, f_2, \dots, f_{N_f}\}, \quad (4.24)$$

де N_f – кількість робочих частот. Псевдовипадковий генератор формує закон перебудови

$$g(n) \in F \quad (4.25)$$

відповідно до якого для групи таймерних елементів вибирається робоча частота f_i . У результаті шумоподібний таймерний сигнал з повільною ППРЧ можна представити у вигляді

$$s(t)_{\text{пов ППРЧ}} = A x_{\text{ТСК}}(t) \cos(\omega(g(n))t + \varphi), \quad (4.26)$$

де A – амплітуда сигналу; $x_{\text{TCK}}(t)$ – таймерна сигнальна конструкція; $\omega(g(n)) = 2\pi f_i$ – миттєва кутова частота; φ – початкова фаза.

На відміну від швидкої ППРЧ, де частота змінюється в межах коротких інтервалів Δ , у повільній ППРЧ одна частота зберігається протягом передачі групи елементів ТСК Δ . Це призводить до формування частотно-часової структури, у якій непозиційна структура ТСК поєднується з псевдовипадковою зміною частотних позицій.

Перевагою такого методу є спрощення реалізації синтезатора частот та системи синхронізації, оскільки перебудова частоти виконується значно рідше. Крім того, зменшуються вимоги до швидкодії приймача та обчислювальних ресурсів системи.

Разом із тим, повільна ППРЧ має нижчу енергетичну прихованість порівняно зі швидкою перебудовою. Оскільки сигнал довше перебуває на одній частоті, підвищується ймовірність його виявлення та постановки вузькосмугової завади. Проте поєднання повільної ППРЧ з таймерним кодуванням частково компенсує цей недолік: непозиційна структура ТСК створює додаткову часову невизначеність, унаслідок чого сигнал залишається складним для аналізу навіть при довшому перебуванні на одній частоті.

Отже, метод повільної ППРЧ для таймерних сигналів базується на передаванні значно більшої групи елементів Δ на одній робочій частоті з подальшою її псевдовипадковою зміною. Такий підхід забезпечує компроміс між структурною прихованістю, завадостійкістю та складністю реалізації системи зв'язку і може застосовуватися в умовах, де критичним є спрощення апаратної реалізації та забезпечення стабільної синхронізації.

4.3.4 Метод багатоканального ППРЧ для таймерних сигналів

Багатоканальний ППРЧ забезпечує одночасне використання декількох частотних каналів для передавання одного інформаційного повідомлення. На відміну від швидкої та повільної ППРЧ, де сигнал у кожний момент часу

передається лише на одній робочій частоті, багатоканальна ППРЧ передбачає паралельне передавання сигналу через множину частотних підканалів. При цьому для кожного інформаційного елемента формується множина робочих частот [37]

$$F_i = \{f_{i1}, f_{i2}, \dots, f_{iw}\}, \quad (4.27)$$

де w – кількість одночасно використовуваних частотних підканалів.

Такий підхід забезпечує зменшення ймовірності втрати інформації під дією вузькосмугових або навмисних завад, оскільки пошкодження окремого частотного каналу не призводить до втрати всього інформаційного символу.

Розглянемо реалізацію багатоканального ППРЧ для таймерних сигналів. Нехай сформована таймерна сигнальна конструкція $x_{\text{ТСК}}(t)$ містить сукупність імпульсних інтервалів, кожний з яких передається одночасно за допомогою декількох робочих частот. Тоді для інтервалу Δ або групі інтервалів із Δ формується множина частот [37]

$$F_{\Delta} = \{f_1, f_2, \dots, f_w\}, \quad (4.28)$$

де w – кількість частот, що використовуються для паралельного передавання.

У цьому випадку кожний часовий елемент Δ дублюється у частотній області, а сигнал набуває просторово-частотної структури. Узагальнена модель багатоканального таймерного сигналу може бути записана у вигляді

$$s(t) = \sum_{j=1}^w A_j x_{\text{ТСК}}(t) \cos(2\pi f_j(t)t + \varphi_j), \quad (4.29)$$

де A_j – амплітуда сигналу в j -му каналі; $f_j(t)$ – псевдовипадкова вибрана частота; φ_j – початкова фаза.

На відміну від швидкої ППРЧ, де перебудова частоти виконується в межах одного або декількох інтервалів Δ , багатоканальна ППРЧ забезпечує одночасне

використання множини частот для одного й того самого фрагмента ТСК. При цьому закон вибору частот може визначатися псевдовипадковою послідовністю $g(t)$, що формує частотний ансамбль

$$F_{\Delta}(g) = \{f_1(g), f_2(g), \dots, f_w(g)\}. \quad (4.30)$$

Кількість часових елементів Δ , що передаються на кожній частоті, визначається як

$$m_f = \frac{1}{w} \left\lfloor \frac{T_f}{\Delta} \right\rfloor, \quad (4.31)$$

де T_f – тривалість використання частотного ансамблю; w – кількість підканалів.

Формула (4.31) показує, що зі збільшенням числа частотних підканалів зменшується навантаження на окрему частоту, а інформація розподіляється між декількома незалежними каналами. Процес формування багатоканального таймерного сигналу можна описати так. Спочатку формується ТСК з параметрами m , s та i . Далі кожний інтервал Δ або їх група відображаються на множину робочих частот відповідно до закону ППРЧ. У результаті утворюється багатоканальний шумоподібний сигнал, у якому часове кодування поєднується з паралельним частотним рознесенням.

Використання непарного числа паралельних частотних підканалів w дозволяє реалізувати мажоритарний принцип прийняття рішення щодо полярності прийнятого елементу Δ [64-67, 85]. У цьому випадку одна й та сама сигнальна реалізація або її копії передаються одночасно через декілька робочих частот, а рішення в приймачі приймається за результатами порівняння полярностей, отриманих у кожному підканалі. Якщо більшість підканалів формує однакове рішення щодо символу («+1» або «-1»), воно вважається правильним. Використання непарного значення w виключає ситуацію рівності голосів між альтернативними рішеннями та забезпечує однозначність декодування. Такий

підхід підвищує завадостійкість системи, особливо в умовах часткового подавлення або спотворення окремих робочих частот навмисними чи випадковими завадами.

Отже, багатоканальний спосіб розширення спектра має ряд переваг:

- 1) підвищення завадостійкості за рахунок дублювання інформації на декількох частотах;
- 2) зменшення впливу вузькосмугових завад;
- 3) підвищення структурної прихованості сигналу;
- 4) ускладнення задачі перехоплення та класифікації сигналу засобами РЕР;
- 5) можливість адаптивного керування кількістю підканалів незалежно від завадової обстановки.

Водночас багатоканальна ППРЧ має певні обмеження. Зі збільшенням кількості частотних каналів зростає потреба у спектральному ресурсі, ускладнюється синхронізація передавача та приймача, а також збільшується апаратна складність системи. Проте для таймерних сигналів цей метод є особливо перспективним, оскільки поєднання непозиційної часової структури ТСК та багаточастотного передавання формує додатковий рівень невизначеності сигналу, що суттєво підвищує його прихованість і стійкість до радіоелектронної протидії.

4.4 Розробка комбінованого методу розширення спектра таймерних сигналів

Одним із перспективних напрямів підвищення прихованості [59, 73, 74] та завадостійкості систем [81-84] радіозв'язку є використання багаторівневих методів формування шумоподібних сигналів. Класичні технології ПРС-ПВП та ППРЧ забезпечують високий рівень енергетичної прихованості та стійкості до навмисних завад, однак переважно орієнтовані на використання позиційних сигнальних конструкцій. У випадку застосування таймерних сигналів виникає можливість реалізації додаткового рівня структурної невизначеності за рахунок непозиційного способу кодування інформації. Це створює передумови для розроблення

комбінованого методу розширення спектра, який одночасно використовує часове, кодове та частотне перетворення сигналу.

Розглянемо багаторівневе перетворенні повідомлення, який поєднує процедури завадостійкого кодування, криптографічного захисту [97-88, 98], таймерного кодування [90] та комбінованого розширення спектра [92, 93, 95, 96]. Загальна структура схема такого перетворення наведена на рис. 4.1. Вона включає блоки завадостійкого кодування, шифрування, формування ТСК, маніпуляції, прямого розширення спектра на основі ПВП, модуляції та ППРЧ. Послідовне виконання зазначених процедур забезпечує багаторівневе перетворення повідомлення перед його передаванням у канал зв'язку.

На початковому етапі інформаційне повідомлення подається у вигляді послідовності розрядно-цифрового коду, що надходить до блоку завадостійкого кодування. Використання коригувальних кодів [19, 86] забезпечує можливість виявлення та виправлення помилок, які виникають у каналі зв'язку під дією випадкових або навмисних завад. Після цього виконується шифрування повідомлення, що забезпечує криптографічний захист передаваних даних та унеможливорює їх змістовне відновлення без знання ключової інформації [73, 98].

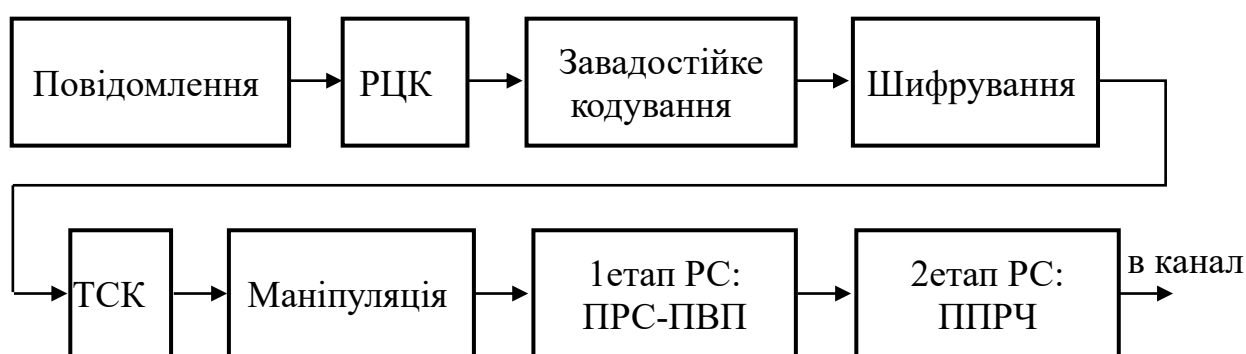


Рис. 4.1. Багаторівневе перетворення повідомлення для формування шумоподібного сигналу

Наступним етапом є формування таймерної конструкції. На відміну від класичних позиційних кодів, де інформація визначається положенням імпульсів у часі t_0 , у ТСК інформаційний зміст задається тривалістю міжімпульсних інтервалів

t_c у межах сигнальної конструкції $T_c = mt_0$. Це дозволяє сформувати сигнал зі змінною часовою структурою t_{ci} та суттєво збільшити число можливих сигнальних реалізацій.

Після побудови ТСК виконується процедура маніпуляції [19, 59]. На цьому етапі параметри таймерного сигналу узгоджуються з обраним видом модуляції, наприклад фазовою маніпуляцією BPSK або QPSK. Особливістю цього процесу є те, що маніпуляція реалізується не лише за рахунок зміни фази або амплітуди, а й шляхом використання часових параметрів ТСК, що забезпечує додатковий рівень структурної прихованості.

Перший рівень розширення спектра реалізується за допомогою методу ПРС–ПВП. Нехай $x_{\text{ТСК}}(t)$ – сформований таймерний сигнал, а $c_{\text{ПВП}}(\tau)$ – псевдовипадкова послідовність, елементи якої мають тривалість, не більшу за дробовий часовий інтервал ТСК. Тоді процес прямого розширення спектра описується співвідношенням [43, 57]

$$x_{\text{рш}}(T_c, \tau) = x_{\text{ТСК}}(T_c, t) \times c_{\text{ПВП}}(\tau), \quad (4.32)$$

де $x_{\text{рш}}(T_c, \tau)$ – таймерний сигнал із розширеним спектром.

Фізично цей процес означає, що кожен елемент таймерного сигналу замінюється групою коротких псевдовипадкових імпульсів тривалістю $\tau \leq \Delta$, які формують широкосмугову структуру сигналу. При використанні прямої або інверсної ПВП зберігається інформація про полярність сигналу та забезпечується можливість його подальшого кореляційного відновлення у приймачі.

Далі послідовність $x_{\text{рш}}(T_c, \tau)$ подається до фазового модулятора для формування шумоподібного сигналу

$$x_{\text{шТСК}}^{\text{фм}}(T_c, \tau) = g(\tau) \cdot \cos(2\pi f_0 \tau + x_{\text{ТСК}}(T_c, \tau)). \quad (4.33)$$

В результаті (4.33) отримуємо шумоподібний сигнал $x_{\text{шТСК}}^{\text{фм}}(T_c, \tau)$ з рівномірним розподілом енергії у широкій смузі частот та автокореляційною

функцією, характерною для широкосмугових сигналів. Далі застосовувався певний метод ППРЧ.

Кількість елементів $N_{\text{ПВП}}(T_c)$ у послідовності розширення $s_{\text{ПВП}}(\tau)$ визначається з урахуванням бази сигналу B_{t_0} на інтервалі t_0 та кількості інтервалів m , що формують таймерну сигнальну конструкцію. За умови $T_c = mt_0$ кількість елементів ПВП на всьому інтервалі формування ТСК визначається як $N_{\text{ПВП}}(T_c) = B_{t_0} \cdot m$. Тут $B_{t_0} = t_0/\tau$ характеризує базу сигналу або коефіцієнт розширення, тобто фактично це кількість елементів ПВП на одному інтервалі t_0 , а τ – тривалість часу двійкового елемента ПВП. Отже, значення $N_{\text{ПВП}}(T_c)$ характеризує загальну кількість елементів розширення, сформованих на повному інтервалі побудови таймерного сигналу T_c . Це означає, що процес прямого розширення спектра для ТСК реалізується не в межах окремого тактового інтервалу t_0 , а на всьому часовому інтервалі сигнальної конструкції T_c .

На рис. 4.2 наведено приклад формування шумоподібного таймерного сигналу ТСК $x_{\text{штскфм}} = (T_c, \tau)$ з параметрами $m = 4$, $s = 4$, $i = 2$ та $B_{t_0} = 16$. Часова структура таймерної конструкції представлена на рис. 4.2 (а). На рис. 4.2 (б) представлена послідовність розширення $s_{\text{ПВП}}(\tau)$ на всьому інтервалі формування ТСК T_c . З урахуванням параметрів B_{t_0} та m кількість імпульсів розширення $N_{\text{тск}} = B_{t_0} \times m = 64$. Процес маніпуляції (ФМ-2) послідовності $x_{\text{рш}}(T_c, \tau)$ надано на рис. 4.2 (д).

Після реалізації ПРС–ПВП здійснюється другий рівень розширення спектра – ППРЧ. На рис. 4.2 (д) представлено процес швидкої ППРЧ. На цьому етапі сформований широкосмуговий таймерний сигнал передається на несучій частоті, яка змінюється відповідно до псевдовипадкового закону. Загальна математична модель такого сигналу може бути подана у вигляді

$$s(\tau)_{\text{шв ППРЧ-ПРС}} = Ax_{\text{штскфм}}^{\text{фм}}(T_c, \tau) \cos(\omega(g(\tau))\tau + \varphi), \quad (4.34)$$

де A – амплітуда сигналу; $x_{\text{ШТСК}}^{\text{фм}}(T_c, \tau)$ – сигнал після процедури ПРС–ПВП; $\omega(g(\tau))$ – миттєва кутова частота, що визначається керуючою псевдовипадковою функцією $g(\tau)$; φ – початкова фаза.

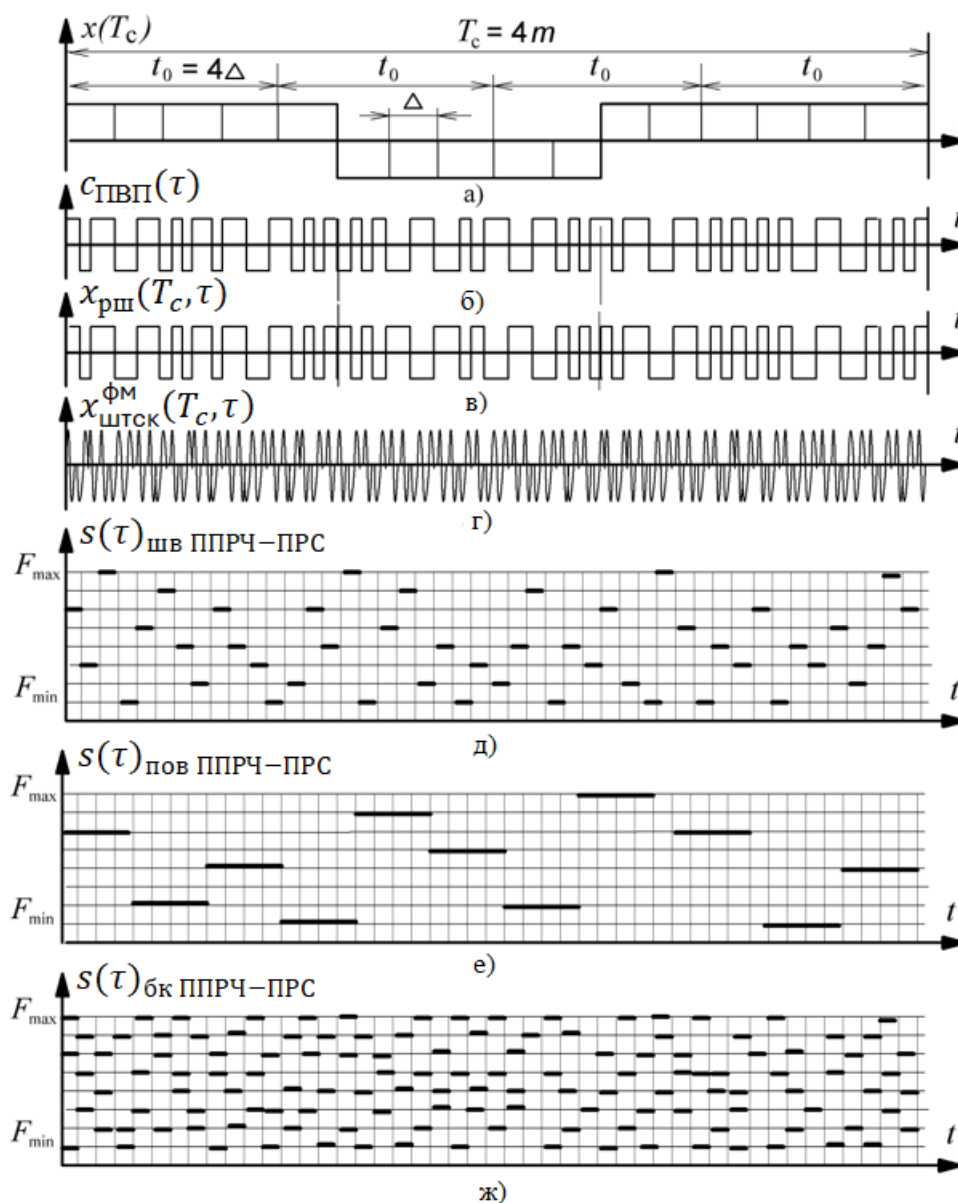


Рис. 4.2. Методи формування шумоподібного таймерного сигналу $x_{\text{ШТСК}}^{\text{фм}}(T_c, \tau)$ на основі комбінованого розширення спектра

Вираз (4.34) описує комбінований шумоподібний сигнал, у якому одночасно реалізуються три незалежні механізми формування невизначеності: таймерне кодування, пряме розширення спектра та псевдовипадковий перескок частоти. У

результаті формується багатовимірною сигнальна структура, яка має складні часові та спектральні характеристики.

На рис. 4.2 (е) надано часові діаграми сигналу $s(\tau)_{\text{пов ППРЧ-ПРС}}$, що сформовані на основі ПРС-ПВП та повільної ППРЧ. Бачимо, що зміна робочої частоти перевищує тривалість однієї або декількох груп елементів Δ .

На рис. 4.2 (ж) надано часові діаграми шумоподібного таймерного сигналу $s(\tau)_{\text{БК ППРЧ-ПРС}}$, що сформовані на основі ПРС-ПВП та багатоканального способу ППРЧ, що передбачає одночасне використання декількох частотних каналів. За рахунок передавання одного елемента на різних робочих частотах цей метод дозволяє підвищити стійкість системи радіозв'язку до завад. Використання непарного числа підканалів, наприклад, $w = 3$ дозволяє реалізувати оцінку якості прийнятого елемента за мажоритарним принципом, що суттєво підвищує завадостійкість системи радіозв'язку. При цьому остаточне рішення про стан прийнятої ТСК буде здійснюватися шляхом визначення приналежності її до підмножини дозволених та недозволених сигнальних конструкцій.

Розроблений комбінований підхід принципово відрізняється від класичних систем ПРС-ПВП і ППРЧ тим, що до класичного кодового та частотного розширення додається ще один рівень невизначеності – таймерна структура сигналу. Якщо у класичних системах шумоподібність формується переважно ПВП або законом перебудови частоти, то у запропонованому методі додатково змінюються часові характеристики сигнальної конструкції. Це забезпечує підвищення структурної прихованості та ускладнює задачу виявлення, синхронізації та класифікації сигналу засобами радіоелектронної розвідки.

4.5 Оцінювання структурної прихованості та інтегральної бази комбінованого сигналу

Одним із ключових критеріїв ефективності шумоподібних сигналів у системах захищеного радіозв'язку є рівень їх структурної прихованості. Для комбінованих сигналів на основі таймерних сигнальних конструкцій цей показник

визначається сукупним впливом часової структури ТСК, псевдовипадкових послідовностей розширення спектра, способу маніпуляції та процедури псевдовипадкового перескоку робочої частоти. На відміну від класичних шумоподібних сигналів, де прихованість формується переважно кодовими або частотними методами, у запропонованому методі використовується багаторівнева невизначеність у просторі параметрів «час–код–частота».

Для кількісної оцінки структурної прихованості комбінованого сигналу використаємо показник

$$S_{\text{ТСК}}^{\text{ПВП-ППрЧ}} = \log_2 N_p + \log_2 N_{\text{ПВП}} + \log_2 N_{\text{см}} + \log_2 N_{\text{ППрЧ}}, \quad (4.35)$$

де N_p – кількість можливих реалізацій таймерних сигналів; $N_{\text{ПВП}}$ – кількість варіантів псевдовипадкових послідовностей; $N_{\text{см}}$ – кількість станів маніпуляції; N_f – кількість можливих частотних позицій при реалізації ППрЧ.

З виразу (4.35) бачимо, що структурна прихованість визначається логарифмом від загальної кількості можливих сигнальних реалізацій. При цьому кожен із компонентів забезпечує незалежний внесок у загальний рівень невизначеності сигналу.

Першою складовою є множина ТСК, яка формується за рахунок параметрів m , s та i . Саме часове кодування забезпечує непозиційний характер сигналу та створює додатковий рівень прихованості ще до застосування класичних методів розширення спектра. Другою складовою виступає ПРС-ПВП, яка реалізує кодове розширення спектра та ускладнює визначення структури сигналу без знання використовуваної псевдовипадкової послідовності.

Особливе значення у комбінованому методі має внесок ППрЧ. Частотний перескок частоти додатково збільшує кількість можливих реалізацій сигналу, оскільки кожен фрагмент ТСК може передаватися на різних робочих частотах. Внесок ППрЧ у структурну прихованість визначається як

$$S_{\text{ППрЧ}} = \log_2(N_f), \quad (4.36)$$

де N_f – характеризує кількість частотних позицій у діапазоні перелаштування.

Збільшення N_f призводить до пропорційного зростання частотної невизначеності та суттєво ускладнює задачу виявлення сигналу засобами радіоелектронної розвідки. Якщо при класичному DSSS противнику достатньо визначити параметри ПВП, то при використанні ППРЧ додатково виникає необхідність відновлення закону зміни частоти, що суттєво збільшує обчислювальну складність аналізу сигналу.

Окрім структурної прихованості, важливим показником комбінованого сигналу є його інтегральна база. Вона характеризує загальний рівень спектрального розширення та визначає потенційну завадостійкість сигналу. Для запропонованого методу інтегральна база визначається як добуток баз окремих способів розширення спектра:

$$B_{\text{комб}} = B_t \times B_f, \quad (4.37)$$

де B_t – база сигналу, сформована методом прямого розширення спектра ПРС-ПВП; B_f – база, яка визначається діапазоном та швидкістю псевдовипадкового перескоку робочої частоти.

Такий підхід відображає комбінований характер формування шумоподібного сигналу. Якщо ПРС-ПВП забезпечує часово-кодове розширення спектра, то ППРЧ додатково розширює сигнал у частотній області. У результаті інтегральна база суттєво перевищує базу окремих методів.

При реалізації ППРЧ структурна прихованість визначається не лише кількістю доступних частотних позицій N_f , але й числом можливих законів їх зміни протягом передавання сигналу. Якщо частотна сітка містить N_f робочих частот, то кількість можливих реалізацій ППРЧ залежить від числа частотних переходів та способу їх формування. Нехай протягом передавання одного шумоподібного сигналу використовується K_f частотних інтервалів перескоку. Тоді загальна кількість можливих частотних реалізацій визначається як

$$N_{\text{ППРЧ}} = N_f^{K_f}, \quad (4.38)$$

де N_f – кількість робочих частот; K_f – кількість частотних переходів або інтервалів перебудови. Формула (4.38) описує випадок, коли кожний інтервал перебудови допускає незалежний вибір будь-якої робочої частоти. У такому випадку внесок ППРЧ у структурну прихованість становить

$$S_{\text{ППРЧ}} = \log_2 (N_f^{K_f}), \quad (4.39)$$

або після перетворення

$$S_{\text{ППРЧ}} = K_f \log_2 N_f. \quad (4.40)$$

Вираз (4.40) показує, що структурна прихованість ППРЧ залежить від двох параметрів: кількості доступних робочих частот N_f ; кількості перебудов частоти K_f . Отже, збільшення кількості частотних позицій або числа перебудов приводить до пропорційного зростання частотної невизначеності.

Для швидкої ППРЧ число частотних переходів визначається відношенням тривалості сигналу до інтервалу перебудови:

$$K_f = \frac{T_c}{T_f}, \quad (4.41)$$

Де T_c – тривалість ТСК; T_f – інтервал роботи на одній частоті.

З урахуванням особливостей таймерних сигналів, де перебудова частоти реалізується в межах одного або кількох інтервалів Δ ,

$$T_f = n_{\Delta} \Delta, \quad (4.42)$$

тоді

$$K_f = \frac{T_c}{n_\Delta \Delta}. \quad (4.43)$$

Оскільки $T_c = mt_0$ та $\Delta = t_0/s$, то кількість частотних переходів для швидкої ППРЧ можна представити через параметри ТСК:

$$K_f = \frac{mst_0}{n_\Delta t_0} = \frac{ms}{n_\Delta}. \quad (4.44)$$

Отриманий вираз є важливим результатом, оскільки безпосередньо пов'язує параметри таймерного кодування з частотною структурою ППРЧ. Тоді кількість можливих законів зміни частоти при швидкій ППРЧ становить

$$N_{\text{ППРЧ}} = N_f^{\frac{ms}{n_\Delta}}. \quad (4.45)$$

З виразу (4.45) випливає, що збільшення параметрів m та s одночасно підвищує часову та частотну складові структурної прихованості. При цьому зменшення кількості інтервалів Δ , протягом яких використовується одна частота (n_Δ), призводить до зростання числа частотних переходів i , відповідно, до збільшення невизначеності частотної структури сигналу.

Виконані розрахунки структурної прихованості шумоподібного таймерного сигналу на основі комбінованого розширення спектра наведено у табл. 4.4. У таблиці представлено вплив параметрів побудови таймерних сигналів m , s , i , а також характеристик псевдовипадкової послідовності розширення спектра та ППРЧ на загальний рівень структурної прихованості комбінованого сигналу.

Аналіз результатів показує, що структурна прихованість формується сукупним внеском часової структури ТСК $S_{\text{ТСК}}$, кодового розширення спектра $S_{\text{ПВП}}$, способу маніпуляції $S_{\text{М}}$ та частотної складової ППРЧ $S_{\text{ППРЧ}}$. При цьому найбільший вплив на загальне значення $S_{\text{ТСК}}^{(\text{пвп-ппрч})}$ має саме частотна складова, що обумовлено великою кількістю можливих законів ППРЧ.

Таблиця 4.4

Структурна прихованість шумоподібного таймерного сигналу на основі комбінованого розширення спектра $S_{\text{ТСК}}^{\text{ПВП-ППрЧ}}$ в залежності від параметрів

№	m	s	i	$S_{\text{ТСК}}$	$S_{\text{ПВП}}$	$S_{\text{М}}$	$S_{\text{ППрЧ}}$	$S_{\text{ТСК}}^{\text{ПВП-ППрЧ}}$
1	4	2	2	4	16	1	32	53
2	4	4	2	5	16	1	80	102
3	6	4	3	9	16	1	120	146
4	7	5	4	12	32	2	210	256
5	8	6	5	15	32	2	288	337
6	9	7	6	18	64	2	378	462
7	10	8	6	21	128	2	480	631

Для першого варіанта ($m = 4, s = 2, i = 2$) сумарна структурна прихованість становить лише 53 дв. вим. У цьому випадку часовий внесок ТСК є відносно невеликим ($S_{\text{ТСК}} = 4$ дв. вим.), а частотна невизначеність ППрЧ забезпечує 32 дв. вим. загальної прихованості. Незважаючи на порівняно помірні параметри, така сигнальна конструкція вже формує достатньо складну структуру для несанкціонованого аналізу.

Подальше збільшення параметра дроблення часового інтервалу s та кількості можливих частотних переходів приводить до суттєвого зростання структурної прихованості. Так, при параметрах $m = 4, s = 4, i = 2$ загальний показник збільшується до 102 дв. вим., тобто

$$S_{\text{ТСК}}^{\text{ПВП-ППрЧ}} = \log_2 45 + \log_2 2^{16} + \log_2 2 + \log_2 32^{16} = 102 \text{ дв. вим.}$$

Таке збільшення пояснюється одночасним збільшенням часової та частотної невизначеності. У цьому випадку внесок ППрЧ уже становить 80 дв. вим.

Отримане значення структурної прихованості $S_{\text{ТСК}}^{\text{ПВП-ППрЧ}} = 102$ дв. вим. означає, що для відновлення структури сигналу при його перехопленні необхідно перевірити приблизно 2^{102} можливих варіантів сигнальних конструкцій. Така кількість реалізацій практично виключає можливість оперативного відновлення

структури сигналу без знання параметрів формування ТСК, ПВП та алгоритму ППРЧ. Високе значення $S_{\text{стр}}$ пояснюється одночасним використанням трьох незалежних рівнів невизначеності: часового, кодового та частотного.

При переході до параметрів $m = 6$, $s = 4$, $i = 3$ структурна прихованість досягає 146 дв. вим.. Зростання параметра m приводить до збільшення кількості реалізацій ТСК та, відповідно, часової складової $S_{\text{тск}}$. Одночасно збільшується кількість інтервалів перебудови частоти, що додатково підвищує значення $S_{\text{ппрч}}$ до 120 дв. вим..

Особливо інтенсивне зростання спостерігається при збільшенні параметрів m , s та довжини ПВП. Для варіантів 4–7 (табл. 4.4) структурна прихованість зростає від 256 до 631 дв. вим.. Зокрема, при $m = 10$, $s = 8$, $i = 6$, $S_{\text{пвп}} = 128$ та внеску ППРЧ 480 дв. вим. загальна структурна прихованість досягає 631 дв. вим.. Це означає, що множина можливих сигнальних реалізацій набуває достатньо великих значень і практично виключає можливість оперативного відновлення структури сигналу без знання параметрів його формування.

Порівняльний аналіз табл. 4.4 свідчить, що зростання структурної прихованості має нелінійний характер. Якщо внесок маніпуляції S_m збільшується відносно повільно, то часово-частотні складові $S_{\text{тск}}$ та особливо $S_{\text{ппрч}}$ демонструють значно швидший приріст. Це пояснюється тим, що збільшення параметрів m та s одночасно впливає як на кількість реалізацій ТСК, так і на число можливих законів зміни робочих частот.

Зростання інтегральної бази $B_{\text{комб}}$ безпосередньо пов'язане зі збільшенням ентропії та шумоподібності сигналу. Чим більшим є значення $B_{\text{комб}}$, тим складніше здійснювати синхронізацію, класифікацію та детектування сигналу стороннім спостерігачем. Водночас надмірне збільшення цього параметра може ускладнювати реалізацію системи зв'язку та висувати жорсткі вимоги до синхронізації передавача і приймача.

4.6 Ентропійний аналіз та адаптивне керування параметрами шумоподібного таймерного сигналу

Одним із важливих показників оцінювання структурної складності та прихованості шумоподібних сигналів є ентропія, яка характеризує ступінь невизначеності або випадковості сигнальної структури. З позицій теорії інформації, запропонований комбінований метод розширення спектра на основі ТСК, ПРС-ПВП та ППРЧ формує багатовимірний сигнальний простір, у якому кількість можливих реалізацій суттєво перевищує аналогічні показники класичних позиційних систем. Відповідно до положень теорії інформації, ентропія джерела повідомлень визначається за формулою К. Шеннона [20]:

$$H = - \sum_{i=1}^n p_i \log_2 p_i, \quad (4.46)$$

де p_i – імовірність появи i -ї сигнальної реалізації; n – кількість можливих станів або сигнальних конструкцій. З наведеної залежності випливає, що ентропія характеризує інформаційну невизначеність системи. При рівноймовірному виникненні всіх сигнальних реалізацій ентропія досягає максимального значення

$$H = \log_2 N, \quad (4.47)$$

де N – загальна кількість можливих сигнальних станів.

Для комбінованого шумоподібного сигналу, сформованого на основі ТСК, ПРС-ПВП та ППРЧ, множина можливих реалізацій визначається параметрами часового кодування, кодового розширення спектра, маніпуляції та частотного перелаштування. У цьому випадку кожна сигнальна конструкція формується як унікальна комбінація параметрів у просторі: «час – частота – код». Така багатовимірна структура принципово відрізняється від класичних шумоподібних сигналів ПРС-ПВП або ППРЧ, де переважає лише один механізм розширення спектра. У запропонованому методі часові параметри ТСК, псевдовипадкові

послідовності та робочі частоти варіюються незалежно, формуючи складний ансамбль сигнальних реалізацій.

За умови статистичної незалежності часових, кодових та частотних процесів ентропію комбінованого сигналу можна подати у вигляді суми окремих складових:

$$H_{\text{комб}} = H_{\text{ТСК}} + H_{\text{ПВП}} + H_{\text{ППРЧ}} + H_{\text{см}}, \quad (4.48)$$

де $H_{\text{ТСК}}$ – ентропія, зумовлена множиною таймерних сигналів; $H_{\text{ПВП}}$ – ентропія кодового розширення спектра; $H_{\text{ППРЧ}}$ – ентропія, обумовлена частотним перелаштуванням; $H_{\text{см}}$ – внесок маніпуляції. Залежність (4.48) свідчить, що комбінований сигнал характеризується значно більшою ентропією порівняно з класичними системами розширення спектра, оскільки формування сигналу відбувається одночасно в декількох незалежних координатах сигнального простору.

Важливим параметром, який визначає ентропійні властивості комбінованого сигналу, є його інтегральна база $V_{\text{комб}} = V_t \times V_f$. Параметр V_t характеризує часово-кодове розширення спектра, сформоване методом ПРС-ПВП, а V_f визначається частотним діапазоном та швидкістю перескоку при ППРЧ. Зростання інтегральної бази $V_{\text{комб}}$ безпосередньо впливає на кількість можливих сигнальних реалізацій та приводить до збільшення ентропії.

При цьому між ентропією та інтегральною базою існує закономірний зв'язок: зі збільшенням $V_{\text{комб}}$ зростає розмірність сигнального простору та експоненційно збільшується число можливих сигнальних станів. Унаслідок цього статистичні характеристики комбінованого сигналу наближаються до властивостей псевдовипадкового процесу, а його структура стає менш передбачуваною для стороннього спостерігача.

Практичне значення цього результату полягає в тому, що великі значення $V_{\text{комб}}$ ускладнюють виконання трьох основних завдань радіоелектронної розвідки: виявлення сигналу; синхронізацію та відновлення його структури; класифікацію і визначення закону формування.

Одночасно надмірне збільшення інтегральної бази може призводити до зростання вимог щодо синхронізації та обчислювальної складності приймача. Тому важливою властивістю запропонованого методу є можливість адаптивного керування параметрами комбінованого сигналу.

Адаптивність реалізується шляхом зміни параметрів ТСК, довжини ПВП та режиму роботи ППРЧ залежно від стану каналу зв'язку та радіоелектронної обстановки. У разі високого рівня навмисних завад доцільним є збільшення значення $B_{\text{комб}}$, що забезпечує підвищення ентропії, структурної прихованості та завадостійкості. За відносно сприятливих умов передавання можливе зменшення бази сигналу для ефективнішого використання частотного ресурсу та зниження енергетичних витрат. Особливу роль у реалізації адаптивного режиму відіграє вибір способу ППРЧ.

Повільний режим ППРЧ передбачає зміну робочої частоти на інтервалі, що перевищує тривалість одного або декількох елементів Δ . Такий підхід спрощує синхронізацію та реалізацію приймача, однак забезпечує обмежений рівень захисту від вузькосмугових і навмисних завад.

Швидкий режим ППРЧ реалізує зміну частоти в межах одного або декількох інтервалів Δ . Це суттєво підвищує ентропію сигналу та ускладнює його виявлення і супроводження засобами радіоелектронної боротьби, але потребує більш точного узгодження передавача і приймача.

Багатоканальний режим ППРЧ передбачає одночасне використання декількох робочих частот. Такий підхід забезпечує просторово-частотне рознесення сигналу, додатково підвищує завадостійкість та може використовуватися у високопродуктивних системах зв'язку.

Таким чином, ентропійний аналіз підтверджує, що комбінований шумоподібний сигнал на основі ТСК, ПРС-ПВП та ППРЧ формує розширений сигнальний простір «час—частота—код» із високим рівнем невизначеності. Зростання інтегральної бази $B_{\text{комб}}$ призводить до підвищення ентропії та структурної прихованості сигналу, а адаптивне керування параметрами ТСК і режимами ППРЧ забезпечує можливість динамічного вибору оптимального

балансу між прихованістю, завадостійкістю та складністю реалізації системи зв'язку.

4.7 Висновки до розділу 4

1. Проведений аналіз параметрів таймерних сигналів показав, що на відміну від позиційних сигналів ТСК формуються за рахунок міжімпульсних інтервалів та характеризуються параметрами m , s та i , які визначають множину допустимих реалізацій сигналу. Збільшення цих параметрів приводить до експоненційного зростання кількості сигнальних конструкцій N_p , що безпосередньо підвищує структурну прихованість.

2. Порівняльний аналіз спектральної та енергетичної ефективності показав, що таймерні сигнали забезпечують вищу частотну ефективність порівняно з позиційними кодами за рахунок більшої інформаційної насиченості часової структури. Це підтвердило доцільність використання ТСК як основи для формування шумоподібних сигналів у системах захищеного радіозв'язку.

3. Розроблено методи розширення спектра таймерних сигналів на основі прямого розширення спектра та псевдовипадкового перескоку робочих частот. Для ППРЧ сформовано алгоритми швидкої, повільної та багатоканальної перебудови частоти, адаптовані до непозиційної структури ТСК, де зміна робочої частоти виконується в межах одного або декількох інтервалів Δ . Це забезпечило можливість інтеграції частотного розширення спектра без втрати властивостей таймерного кодування.

4. Показано, що структурна прихованість комбінованих шумоподібних сигналів визначається сукупною дією часового, кодового та частотного рівнів невизначеності та може бути оцінена як: $S_{\text{стр}} = \log_2(N_p N_{\text{ПВП}} N_{\text{см}} N_{\text{ППРЧ}})$. Встановлено, що внесок ППРЧ визначається не лише кількістю доступних частот N_f , але і кількістю частотних перестроювань у межах сигналу, що формує множину можливих частотних траєкторій.

5. Аналіз залежності структурної прихованості від параметрів ТСК, ПВП та ППРЧ показав її експоненційне зростання зі збільшенням параметрів формування сигналу та бази методів розширення спектра. Для прикладу при $m = 4$, $s = 4$, $i = 2$, $N_{\text{ПВП}} = 2^{16}$, $N_f = 32$ та двійковій маніпуляції отримано структурну прихованість близько 102 біт, що відповідає приблизно 2^{102} можливим реалізаціям сигналу.

6. Встановлено, що збільшення інтегральної бази комбінованого сигналу $B_{\text{комб}} = B_t \times B_f$ призводить до підвищення ентропії, шумоподібності та завадозахищеності сигналу, ускладнюючи його виявлення, класифікацію та відновлення сторонніми засобами спостереження. Водночас надмірне збільшення бази сигналу підвищує вимоги до синхронізації та апаратної реалізації системи зв'язку, що потребує адаптивного вибору параметрів розширення спектра залежно від умов функціонування системи.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-технічне завдання підвищення прихованості передавання інформації в інформаційно-комунікаційних системах шляхом інтеграції таймерних сигнальних конструкцій із методами псевдовипадкового перескоку робочих частот для формування комбінованих шумоподібних сигналів із підвищеною структурною невизначеністю та стійкістю до виявлення і перехоплення.

У результаті проведених досліджень отримано такі основні результати:

1. Проведено аналіз існуючих методів забезпечення прихованості передавання інформації в умовах радіоелектронної протидії. Встановлено, що застосування лише одного механізму розширення спектра (ПРС-ПВП або ППРЧ) формує структурну прихованість у межах 16–128 дв. вим. та 32–480 дв. вим. відповідно, тоді як їх інтеграція з таймерними сигнальними конструкціями забезпечує формування додаткового часового рівня невизначеності.

2. Досліджено особливості формування таймерних сигнальних конструкцій та встановлено, що використання непозиційного принципу кодування забезпечує збільшення структурної прихованості на 4–21 дв. вим. залежно від параметрів побудови сигналу ($m = 4 \dots 10$, $s = 2 \dots 8$, $i = 2 \dots 6$), що створює додатковий часовий рівень невизначеності порівняно з позиційними кодами.

3. Досліджено спектральні, статистичні та кореляційні властивості таймерних сигнальних конструкцій. Встановлено залежність між кодовою відстанню та коефіцієнтами взаємної кореляції сигналів. Показано, що при збільшенні кодової відстані від 1Δ до 7Δ коефіцієнти взаємної кореляції зменшуються від 0,882–0,870 до 0,149–0,078, що підтверджує можливість формування слабокорельованих ансамблів сигналів із мінімальною кодовою відстанню $d_{\text{мшт}}(\Delta) > 1$.

4. Проведено оцінювання кореляційних властивостей ансамблю таймерних сигнальних конструкцій, для якого проаналізовано парні комбінації сигналів.

Встановлено, що середній коефіцієнт взаємної кореляції становить $\bar{r} \approx 0,64$, а коефіцієнт ортогональності – Корт $\approx 0,36$, що підтверджує можливість використання ТСК для формування шумоподібних сигналів із помірним рівнем взаємної незалежності.

5. Розроблено методи інтеграції таймерних сигнальних конструкцій із технологіями прямого розширення спектра та псевдовипадкового перескоку робочих частот. Запропоновано алгоритми реалізації швидкої, повільної та багатоканальної ППРЧ, які забезпечують формування комбінованих часово-частотно-кодкових сигналів із кількістю можливих частотних реалізацій $N_{\text{ППРЧ}} = N_f^{ms/n_\Delta}$, що дозволяє експоненційно збільшувати структурну прихованість сигналів зі зростанням параметрів m та s .

6. Розроблено математичний апарат оцінювання структурної прихованості комбінованих сигнально-кодкових конструкцій. Встановлено, що структурна прихованість комбінованих сигналів зростає експоненційно зі збільшенням кількості часових, кодкових і частотних реалізацій та для досліджених параметрів досягає 631 дв. вим., що відповідає множині можливих реалізацій порядку 2^{631} .

7. Встановлено кількісний внесок окремих складових у формування структурної прихованості комбінованих сигналів. Показано, що внесок таймерних сигнальних конструкцій становить 4–21 дв. вим., внесок прямого розширення спектра – 16–128 дв. вим., внесок псевдовипадкового перескоку робочих частот – 32–480 дв. вим.. При цьому загальна структурна прихованість комбінованих сигналів зростає від 53 до 631 дв. вим., що підтверджує визначальний вплив частотної складової на загальний рівень структурної невизначеності сигналу.

Отримані результати становлять теоретичну та практичну основу для створення перспективних систем захищеного радіозв'язку з підвищеним рівнем прихованості передавання інформації та можуть бути використані під час розроблення спеціалізованих інформаційно-комунікаційних систем, що функціонують в умовах радіоелектронної протидії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз завадозахищених режимів роботи сучасних військових УКХ радіостанцій тактичної ланки управління та практичні рекомендації щодо їх використання / В. А. Ченченко, В. І. Руденко, Л. О. Бондаренко, М. О. Зінченко. *Системи і технології зв'язку, інформатизації та управління*. 2022. № 1. С. 106–115. DOI: <https://doi.org/10.58254/viti.1.2022.10.81>
2. Іохов О. Ю. Захист радіомереж підрозділів Національної гвардії України від радіотехнічної розвідки : монографія. Харків : НА НГУ, 2017. 222 с.
3. Манько А. В. (2024) Метод адаптації системи радіозв'язку в умовах активного застосування засобів радіоелектронної боротьби. *Честь і закон*. № 2. 88–95.
4. Serkov A. A., Kasilov O. V., Lazurenko B. O., Pevnev V. Y., Trubchaninova K. A. (2023) Strategy of building a wireless mobile communication system in the conditions of electronic counteraction. *Radioelectronic and computer systems*. No. 2 (106). 160–170. – Режим доступу: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/93493>.
5. Король, Я., Степанов, В., & Петренко, Ю. (2024). Рекомендації щодо забезпечення зв'язку в умовах застосування противником засобів радіоелектронної боротьби. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №5(5), 45–56. – Режим доступу: <http://perspectives.pp.ua/index.php/niu/article/view/17627/17689>
6. Бібік, А. В., Городиський, Р. О., Ваврічен, О. А., & Степанов, В. О. (2026). Підвищення стійкості оперативного радіозв'язку в умовах сучасних загроз: потенціал мереж TETRA для підрозділів сектору безпеки та оборони й органів охорони державного кордону України. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №1(18), 69–83. – Режим доступу: [https://doi.org/10.52058/3041-1793-2026-1\(18\)-69-83](https://doi.org/10.52058/3041-1793-2026-1(18)-69-83)
7. TETRA Association. Security and Encryption in TETRA Networks: White Paper. –London: TCCA, 2022. –54 p.

8. Дослідження застосування радіостанцій “Himera” G1 Pro та ретранслятора B1 у бойовій системі “Кропива”, з метою покращення спроможностей автоматизованих систем тактичної ланки управління/ Юрій ПЕТРЕНКО, Ігор ШЕВЕЛЬОВ, Вадим СТЕПАНОВ// Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану// Військова академія (м. Одеса)/ Збірник тез доповідей VII Міжнародної науково-практичної конференції 17 жовтня 2025 року. Секція 11. Актуальні проблеми безпеки та оборони в умовах сучасних воєнних конфліктів – с. 515-516. – Режим доступу: <https://vaodesa.mil.gov.ua/wp-content/uploads/2025/12/zbirnyk.pdf>

9. ETSI EN 300 392-2.Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI). v3.8.1, 2022.

10. Dunlop J., Girma D., Irvine J. Digital Mobile Radio Systems: A Comprehensive Treatment of Civil and Professional Radio Systems. Wiley, 2019. 464 p.

11. Конахович Г. Ф., Пузиренко О. В. Криптографічні методи захисту інформації в цифрових системах зв'язку. –К.: НАУ, 2020. –280 с.

12. 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.

13. 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.

14. Степаненко О. В., Адрієвський Р. С. Аналіз завадостійкості цифрових систем зв'язку в умовах впливу навмисних завад // Збірник наукових праць ВІТІ. – 2023. – No 2. –С. 45–56.

15. Proakis, J. G., & Manolakis, D. K. Digital Signal Processing: Principles, Algorithms, and Applications. – 4th ed. – Upper Saddle River, NJ: Prentice Hall, 2007. – 1002 p.

16. Sklar, B. Digital Communications: Fundamentals and Applications. – 2nd ed. – Upper Saddle River, NJ: Prentice Hall, 2001. – 1100 p.

17. Сайко В. Г., Стеклов В. П. Проектування мереж радіозв'язку: Підручник для ВНЗ. –К.: Техніка, 2021. –320 с.

18. Захарченко М.В., Корчинський В.В, Радзімовський Б.К., Горохов Ю.С. (2015) Ефективність прямого розширення спектра в системах зв'язку з таймерними сигналами. Вісник НУ «Львівська політехніка». № 818. 76-79.

19. Захарченко М.В. Системи передавання даних / М.В.Захарченко М.М. Гаджиев, В.Є. Басов, О.М. Мартинова та ін. // – Т.1: Завадостійке кодування: підручник [для студ. вищ. техн. навч. закл.]. / – Одеса «Фенікс», 2009. – 406 с.

20. Shannon, C. E. A Mathematical Theory of Communication. – University of Illinois Press, 1948. – 144 pp.

21. Poisel, R. A. Modern Communications Jamming: Principles and Techniques. Boston: Artech House, 2011. 450 p. – Режим доступу: <https://scispace.com/pdf/modern-communications-jamming-principles-and-techniques-3hfzjoioldw.pdf>

22. Нагорнюк О. А. Метод автоматичного визначення часових параметрів радіосигналів із псевдовипадковим перестроюванням робочої частоти на фоні вузькосмугових перешкод. Збірник наукових праць ЖВІ. 2018. Вип. 15. С. 53–64.

23. Кривенко О. В. Методика формування сигналу в радіозасобах з ППРЧ в умовах впливу навмисних шумових завад. Системи озброєння і військова техніка. 2017. № 1 (49). С. 132–135. – Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2017_1_27

24. Гурський Т. Г. Підвищення завадозахищеності радіоліній з ППРЧ в умовах завад у відповідь. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3 (40). С. 58–62. – Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_3_15

25. Гурський Т. Г., Кривенко О. В. Методика формування сигналу в радіозасобах з ППРЧ при передачі мови в умовах впливу завад у відповідь. Системи управління, навігації та зв'язку. 2017. Вип. 2 (42). С. 179–184. – Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2017_2_46

26. Гурський Т.Г., Жук О.Г., Кривенко О.В., Шишацький А.В. (2016) Напрямки вдосконалення засобів радіозв'язку з псевдовипадковою перестройкою робочої частоти : *Збірник наукових праць ВІПІ*. Вип. 1. 25-34.

27. Шишацький А. В., Кувшинов О. В., Петрунчак С. П. (2017) Методика вибору раціональних значень параметрів багатоантенних систем військового радіозв'язку з псевдовипадковою перестройкою робочої частоти. Системи озброєння і військова техніка. № 2 (50). 151–155. – Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2017_2_34

28. Кувшинов О. В., Шишацький А. В., Жук О. Г., Беляков Р. О., Прокопенко Є. М., Леонт'єв О. Б., Животовський Р. М., Дробаха Г. А., Романенко І. О., Петрук С. М. (2019) Розробка методики підвищення завадозахищеності засобів радіозв'язку з псевдовипадковою перестройкою робочої частоти : *Східно-Європейський журнал передових технологій*. Том 2, № 9 (98): Інформаційно-керуючі системи. 74–84.

29. Семененко О. М., Бойко Р. В., Добровольський Ю. Б., Іванов В. Л., Кремешний О. І. (2016) Контррадіоелектронна боротьба як складова частина радіоелектронної боротьби в Збройних Силах України // Системи озброєння і військова техніка. № 2. 141-145. – Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2016_2_31

30. Наконечний Т. А., & Євграфов Д. В. Перехоплення сигналу витoku інформації з екрану монітора. Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи» : матеріали конференції, 19-25 березня 2018 р., м. Київ, Україна / КПП ім. Ігоря Сікорського, РТФ. – Київ : КПП ім. Ігоря Сікорського, 2018. – С. 279–281. – Режим доступу: <https://ela.kpi.ua/handle/123456789/38000>

31. 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. – Режим доступу: http://nbuv.gov.ua/UJRN/Mtkm_tekh_2019_19_8

32. Лізунов С. І., Кадулін М. О. Використання аналізаторів спектра для захисту інформації. Тиждень науки-2019 : *фах. радіоелектроніки та телекомунікацій* : збірник тез доп. щоріч. наук.-практ. конф. (Запоріжжя, 15–19 квітня 2019 р.). Запоріжжя : ЗНТУ, 2019. С. 110–112.

33. Adamy D. L. EW 101: A First Course in Electronic Warfare. Boston : Artech House, 2001. 320 p.

34. Knott, E. F., Shaeffer, J. F., Tuley, M. T. Radar Cross Section. 2nd ed. Boston: Artech House, 2004. 611 p.

35. Політанський, Р.Л. Енергетична ефективність широкосмугової системи, що використовує фрактальні сигнали / Р.Л. Політанський // VI Міжнародний науково-технічний симпозиум «Новые технологии в телекоммуникациях». – Киев, Украина. – Січень, 2013. С. 60-63.

36. Горохов Ю.С. Метод кодового розділення каналів на основі таймерних сигнальних конструкцій / Ю.С. Горохов, Корчинський, Е.М. Рудий // Міжнародний науково-технічний журнал Вимірювальна та обчислювальна техніка в технологічних процесах. – 2016. – №1 – С.208-211.

37. Корчинський В.В. Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів / Корчинський В.В., Назаренко О.А., Степанов В.О., Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». № 2 (02) 2022, - С.25-31.

38. 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.

39. 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.

40. Корчинський В.В., Кільдішев В.Й., Степанов В.О., Богданюк І.А., Ярема В.В., Поліщук О.В., Бельська І. С. Комбінований метод захисту інформації на основі криптографічних алгоритмів, завадостійких кодів та методів розширення спектра. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. 317-321.

41. Мандзій, Б. А. Основи теорії сигналів / Б.А. Мандзій, Р.І. Желяк // Підручник. За ред. Б.А. Мандзія. Львів: Видавничий дім «Ініціатива». — 2008. — 240 с.

42. 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.

43. 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.

44. 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.

45. Математичні основи оптимізації телекомунікаційних систем: підручник. За загальною редакцією Захарченко М.В. / Захарченко М.В., Горохов С.М., Балан М.М., Гаджієв М.М., Корчинський В.В., Ложковський А.Г. Одеса: ОНАЗ ім. О.С. Попова, 2010. – 240 с.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

59. 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.

60. Korchynskyi, V., Kildishev, V., Bektursunov, D., Havel, S., Stepanov, V., Slavych, V., & Petrovskyi, R. (2026). Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. *Technology Audit and Production Reserves*, №1(87), 18–24. – Режим доступу: <https://doi.org/10.15587/2706-5448.2026.353067>

61. 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.

62. 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.

63. Гавель, С., Корчинський, В., Степанов, В., & Куртіков, М. (2026). Методи підвищення криптографічної стійкості псевдовипадкових послідовностей на основі генераторів хаосу. *Herald of Khmelnytskyi National University. Technical Sciences*, 363(2), 149–154. – Режим доступу: <https://doi.org/10.31891/2307-5732-2026-363-19>

64. Korchynskiy, V., Havel, S., Sevastieiev, Ye., Petrovskiy, R., Slavych, V., Stepanov, V., & Riabukha, O. (2026). Methods of forming noise-like signals based on chaotic sequences and spline approximation. *Advances in Cyber-Physical Systems*, Vol. 11, No. 11, 50–55. Lviv Polytechnic National University. – Режим доступу: <https://doi.org/10.23939/acps2026.01.050>.

65. 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.

66. 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.

67. 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.

68. Корчинський, В., Рябуха, О., Степанов, В., Голев, Д., & Лімарь, І. (2025). Пристрій захисту мовного акустичного сигналу в умовах радіоелектронної боротьби. *Measuring and Computing Devices in Technological Processes*, 82(2), 187–192. – Режим доступу: <https://doi.org/10.31891/2219-9365-2025-82-25>

69. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення – 02.11.2023).

70. Боднар І. Р. "Інформаційна безпека як основа національної безпеки." *Mechanism of Economic Regulation* 1 (2014): с. 68-75.

71. Гнатюк С. О., Рябий М. О., & Лядовська В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв'язок*, (4), 3-7.

72. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах НД від несанкціонованого доступу [Електронний ресурс] / Затверджено наказом № 22 ДСТСЗІ СБУ від 28.04.1999. – 57 с. – Режим доступу: <https://tzi.com.ua/downloads/2.5-004-99.pdf>.

73. Лунтовський А.О. Мультисервісні мобільні платформи / А.О. Лунтовський, М.В. Захарченко, А.І. Семенко – К.: ПВП «Задруга», 2014. – 214 с.

74. Протоколи, термінальне обладнання та інформаційна безпека у мережах наступного покоління: [навч. посібник] / М. В. Захарченко, О.О. Вараксін, В.Г. Кононович, С.О. Вараксін; за ред. М. В. Захарченка. – Одеса: Фенікс, 2008. – 128 с.

75. Корчинський В.В. Прогнозування та оцінки ризиків інсайдерських загроз / Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П. //«Перспективні напрями захисту інформації : Матеріали шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С.64-65.

76. Корчинський В.В. Мінімізація ризиків інсайдерських загроз в системах захисту /В.В. Корчинський, Аль-Файюми Халед // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. Ч.І., Одеса, 12-14 грудня. – 2019. – С. 139.

77. Корчинський В.В. Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// Наукові праці ОНАЗ ім. О. С. Попова – Одеса: ОНАЗ, 2019, № 2. – С. 112-116.

78. Політанський, Л.Ф. Система передавання даних з використанням генераторів хаосу [Текст] / С. Д. Галюк, Л.Ф. Політанський, О. В. Гресь, Р. Л. Політанський // Радиотехника, 2011. – №164. – С. 66-71.

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

80. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – Р. – 65-69.

81. 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.

82. Захарченко М.В. Порівняння синдромних методів для коригуючих блокових позиційних і таймерних кодів / М.В. Захарченко, М.М. Гаджієв, Б.К. Радзімовський, Ю. С. Горохов, Д. О. Шпак // Восточно-Европейский журнал передовых технологий. – 2014. – № 2/9(68). – С. 4–8.

83. Volodymyr Korchynskyi, Valerii Hordiichuk, Vitalii Kildishev, Oleksandr Riabukha, Sergii Staikutsa, Khaled Alfaiomi. Method of information protection based on

the integration of probabilistic encryption and noise immune coding. – Radioelectronic and computer systems, 2023.4.13, P.184-185.

84. 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), October 26, 2021, Kyiv, Ukraine. CEUR Workshop Proceedings. 2022. P. 182-194.

85. Корчинський В.В. Ефективність j -кратного повторення надлишкових таймерних сигнальних конструкцій / В.В. Корчинський, В.Й. Кільдішев, С.В. Хомич, Ю.В. Белова // Вестник НТУ «ХПИ». – Харьков: ХПИ, 2012. – Вип. 26. – С. 88-95.

86. Корчинський В.В. Ефективність трансформації швидкості передачі в нову якість у каналах зв'язку з моделлю Гільберта / В.В. Корчинський, В.Й. Кільдішев, М.М. Гаджієв // Наукові праці ОНАЗ ім. О. С. Попова, 2009, № 1. – С. 92–95.

87. Haykin, S. Communication Systems. – 5th ed. – Hoboken, NJ: John Wiley & Sons, 2009. – 608 p.

88. Lathi, B. P., & Ding, Z. Modern Digital and Analog Communication Systems. – 4th ed. – New York, NY: Oxford University Press, 2009. – 964 p.

89. Hsu, H. P. Schaum's Outline of Signals and Systems. – 3rd ed. – New York, NY: McGraw-Hill Education, 2014. – 504 p.

90. Захарченко М.В. Статистичні параметри спотворень таймерних сигнальних конструкцій в каналах моделі Гільберта / М.В. Захарченко, О.М.Мартінова, Ю.С. Горохов, Д.Н. Бектурсунов, А.С. Кріль // Збірник наукових праць ОНАЗ ім. О. С. Попова. –2015. – № 1. – С. 42–47.

91. Степанов В.О., Петренко Ю.А., Корчинський В.В., Назаренко О.А. Підвищення завадозахищеності систем зв'язку на основі розширення спектра таймерних сигналів. Науково-технічна конференція 'Системи і технології зв'язку, інформатизації та кібербезпеки: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 1 грудня 2022 року Київ. 2022. 202-203

92. Корчинський В.В. Підвищення прихованості передавання шумоподібних

сигнально-кодових конструкцій на основі таймерних сигналів / В.В. Корчинський, В.О. Степанов // Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. К.: НУОУ, 2023. 84-87.

93. Корчинський В.В. Методи захисту інформації на основі розширення спектра сигналу / В.В. Корчинський, О. М. Рябуха, Ю. В. Белова, Степанов В.О. // VII International Scientific and Practical Conference «Scientific Paradigm in the Context of Technologies and Society Development» held on July 16-18, 2024 in Geneva, Switzerland, 216-220. – Режим доступу: <https://archive.interconf.center/index.php/conference-proceeding/issue/view/16-18.07.2024>

94. Bielova Iuliia, Stepanov Vadym, Bohdaniuk Ihor, Manankov Roman. Intelligent ai-based siem systems for detection and analysis of cyber incidents // Development of science in the XXI century. Proceedings of the V International Scientific and Practical Conference. Marseille. France. 2025. 159-160. – Режим доступу: <https://conference-w.com/wp-content/uploads/2026/01/Fra.M-2526122025.pdf>

95. 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. С. 543.

96. Корчинський В.В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції / Корчинський В.В., Рябуха О. М., Бердніков О.М., Аль-Файюми Халед, Поліщук К.В.// Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня - 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 27-30.

97. V. Hordiichuk, V. Korchynskyi, V. Kildishev, B. Molodetskyi, S. Staikutsa and K. Alfaioni, "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, pp. 1-4.

98. Голдвассер С., Мікалі С. Криптографія та теорія обчислень. – К.: Видавництво «Наукова думка», 2016. – 320 с.

ДОДАТОК А

ПЕРЕЛІК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Корчинський, В. В., Назаренко, О. А., Степанов, В. О., & Аль-Файюми, Х. (2022). Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів. *Інфокомунікаційні та комп'ютерні технології*, №2(02), 25–31. Київ: Відкритий міжнародний університет розвитку людини «Україна». Retrieved from <https://visn-icct.uu.edu.ua/index.php/icct/article/download/86/70>
2. Korchynskiy, V., Kildishev, V., Bektursunov, D., Havel, S., Stepanov, V., Slavych, V., & Petrovskiy, R. (2026). Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. *Technology Audit and Production Reserves*, №1(87), 18–24. <https://doi.org/10.15587/2706-5448.2026.353067> (Scopus)
3. Гавель, С., Корчинський, В., Степанов, В., & Куртіков, М. (2026). Методи підвищення криптографічної стійкості псевдовипадкових послідовностей на основі генераторів хаосу. *Herald of Khmelnytskyi National University. Technical Sciences*, 363(2), 149–154. <https://doi.org/10.31891/2307-5732-2026-363-19>
4. Korchynskiy, V., Havel, S., Sevastieiev, Ye., Petrovskiy, R., Slavych, V., Stepanov, V., & Riabukha, O. (2026). Methods of forming noise-like signals based on chaotic sequences and spline approximation. *Advances in Cyber-Physical Systems*, Vol. 11, No. 11, 50–55. Lviv Polytechnic National University. <https://doi.org/10.23939/acps2026.01.050>
5. Корчинський, В., Рябуха, О., Степанов, В., Голев, Д., & Лімарь, І. (2025). Пристрій захисту мовного акустичного сигналу в умовах радіоелектронної боротьби. *Measuring and Computing Devices in Technological Processes*, 82(2), 187–192. <https://doi.org/10.31891/2219-9365-2025-82-25>
6. Король, Я., Степанов, В., & Петренко, Ю. (2024). Рекомендації щодо забезпечення зв'язку в умовах застосування противником засобів радіоелектронної боротьби. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №5(5), 45–56. Retrieved from

<http://perspectives.pp.ua/index.php/niu/article/view/17627/17689>

7. Бібік, А. В., Городиський, Р. О., Ваврічен, О. А., & Степанов, В. О. (2026). Підвищення стійкості оперативного радіозв'язку в умовах сучасних загроз: потенціал мереж TETRA для підрозділів сектору безпеки та оборони й органів охорони державного кордону України. *Національні інтереси України: Воєнні науки, національна безпека, безпека державного кордону*, №1(18), 69–83. [https://doi.org/10.52058/3041-1793-2026-1\(18\)-69-83](https://doi.org/10.52058/3041-1793-2026-1(18)-69-83)

Наукові праці, які засвідчують апробацію матеріалів дисертації:

8. 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. 17–18.

9. Степанов В.О., Петренко Ю.А., Корчинський В.В., Назаренко О.А. Підвищення завадозахищеності систем зв'язку на основі розширення спектра таймерних сигналів. Науково-технічна конференція 'Системи і технології зв'язку, інформатизації та кібербезпеки: Військовий інститут телекомунікацій та інформатизації імені Герої Крут, 1 грудня 2022 року Київ. 2022. 202-203. – Режим доступу: <https://mitit.mil.gov.ua/api/files/2173>

10. Корчинський В.В. Підвищення прихованості передавання шумоподібних сигнально-кодів конструкцій на основі таймерних сигналів / В.В. Корчинський, В.О. Степанов // Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. К.: НУОУ, 2023. 84-87. – Режим доступу: <https://drive.google.com/file/d/1VpULkcweKcyZ-KR8EvxtxQSGYbyS1JSq/view>

11. Корчинський В.В. Методи захисту інформації на основі розширення спектра сигналу / В.В. Корчинський, О. М. Рябуха, Ю. В. Белова, Степанов В.О. // VII International Scientific and Practical Conference «Scientific Paradigm in the Context of Technologies and Society Development» held on July 16-18, 2024 in Geneva, Switzerland, 216-220. – Режим доступу: <https://archive.interconf.center/index.php/conference-proceeding/issue/view/16-18.07.2024>

12. Bielova Iuliia, Stepanov Vadym, Bohdaniuk Ihor, Manankov Roman. Intelligent ai-based siem systems for detection and analysis of cyber incidents // Development of science in the XXI century. Proceedings of the V International Scientific and Practical Conference. Marseille. France. 2025. 159-160. DOI <https://doi.org/10.5281/zenodo.18115841>

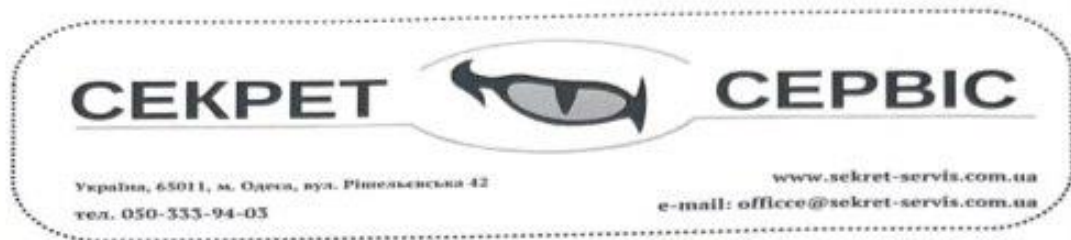
13. Корчинський В.В., Кільдішев В.Й., Степанов В.О., Богданюк І.А., Ярема В.В., Поліщук О.В., Бельська І. С. Комбінований метод захисту інформації на основі криптографічних алгоритмів, завадостійких кодів та методів розширення спектра. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. 317-321. – Режим доступу: <https://suitt.edu.ua/wp-content/uploads/2026/03/zbirnyk-tez-duitz-80-mntk.pdf>

14. Дослідження застосування радіостанцій “Нимера” G1 Pro та ретранслятора В1 у бойовій системі “Кропива”, з метою покращення спроможностей автоматизованих систем тактичної ланки управління/ Юрій ПЕТРЕНКО, Ігор ШЕВЕЛЬОВ, Вадим СТЕПАНОВ// Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану// Військова академія (м. Одеса)/ Збірник тез доповідей VII Міжнародної науково-практичної конференції 17 жовтня 2025 року. Секція 11. Актуальні проблеми безпеки та оборони в умовах сучасних воєнних конфліктів – с. 515-516. – Режим доступу: <https://vaodesa.mil.gov.ua/wp-content/uploads/2025/12/zbirnyk.pdf>

15. 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. С. 543. – Режим доступу: <https://impeer.org.ua/wp-content/uploads/2025/07/%D0%9C%D0%9E%D0%9D%D0%9E%D0%93%D0%A0%D0%90%D0%A4%D0%86%D0%AF-26-06-2024.pdf>

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ



АКТ ВПРОВАДЖЕННЯ

результатів дисертаційної роботи «Підвищення прихованості передавання широкосмугових таймерних сигналів на основі псевдовипадкового перескоку робочої частоти» на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека
Степанова Вадима Олександровича

Комісія у складі в. о. директора ТОВ «БФ «Секрет Сервіс» Мирошніченка Олександра Михайловича та директора сервісної служби Матей Марії Олександрівни.

Розглянувши результати дисертаційної роботи «Підвищення прихованості передавання широкосмугових таймерних сигналів на основі псевдовипадкового перескоку робочої частоти», підтверджуємо, що основні наукові та практичні результати можуть застосовуватися в діяльності підприємства ТОВ «БФ «Секрет Сервіс».

Зокрема, інтерес для практичного використання становлять такі розробки:

- метод підвищення захищеності інформаційного обміну в інформаційно-комунікаційних системах на основі інтеграції таймерних сигнальних конструкцій, прямого розширення спектра та псевдовипадкового перескоку робочих частот, який забезпечує підвищення прихованості передавання інформації та ускладнює її виявлення, аналіз і перехоплення;
- метод формування комбінованих широкосмугових шумоподібних сигналів на основі таймерних сигнальних конструкцій, який забезпечує реалізацію швидкої, повільної та багатоканальної перебудови робочих частот без втрати властивостей непозиційного таймерного кодування;
- аналітичні залежності структурної прихованості від параметрів таймерних сигнальних конструкцій, псевдовипадкових послідовностей та алгоритмів псевдовипадкового перескоку робочих частот, що дозволяють прогнозувати рівень захищеності інформаційного обміну та обґрунтовувати вибір параметрів формування сигналів;

В. о. директора

ТОВ «БФ «Секрет Сервіс» _____



Мирошніченко О. М.

Директор сервісної служби _____

Матей М. О.

ЗАТВЕРДЖУЮ

Проректор з навчальної роботи
Державного університету інтелектуальних
технологій і зв'язку

проф. д-р. наук з держ. управ.

С. К. Хаджиралєва

« 24 » березня 2026 року

АКТ

впровадження результатів дисертаційної роботи

Степанова Вадима Олександровича

на тему:

**«Підвищення прихованості передавання широкосмугових таймерних сигналів на основі
псевдовипадкового перескоку робочої частоти»**

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.; д.т.н., доц. каф. КБ та ТЗІ Кільдішев В.Й.; к.ф.н., доц.
каф. КБ та ТЗІ Стайкуца С.В.; секретар каф. КБ та ТЗІ, Дунаєва В.В. склали цей акт про таке.

Результати дисертаційної роботи здобувача кафедри кібербезпеки та технічного захисту
інформації Степанова Вадима Олександровича на тему «Підвищення прихованості передавання
широкосмугових таймерних сигналів на основі псевдовипадкового перескоку робочої частоти»
впроваджено в освітній процес Державного університету інтелектуальних технологій і зв'язку.

Наукові результати дисертаційної роботи використовуються під час викладання
дисциплін «Забезпечення кібербезпеки у Збройних Силах України» та «Теоретичні основи
передавання та захисту інформації», зокрема в розділах, присвячених методам підвищення
прихованості передавання інформації в системах радіозв'язку, застосуванню таймерних
сигнальних конструкцій, технологіям прямого розширення спектра сигналів, псевдовипадкового
перелаштування робочих частот, а також оцінюванню структурної прихованості
широкосмугових шумоподібних сигналів в умовах радіоелектронної протидії.

Отримані результати сприяють підвищенню якості підготовки здобувачів вищої освіти за
спеціальністю 125 «Кібербезпека», розширюють навчально-методичне забезпечення дисциплін
професійної підготовки та використовуються при виконанні науково-дослідних робіт у сфері
захисту інформації та кібербезпеки.

Голова комісії:

Декан факультету ІТК ДУІТЗ,
д.т.н., проф.

Члени комісії:

д.т.н., проф., зав. каф. КБ та ТЗІ
д.т.н., доц. каф. КБ та ТЗІ
к.ф.н., доц. каф. КБ та ТЗІ
секретар каф. КБ та ТЗІ



Васіліу Є.В.



Корчинський В.В.

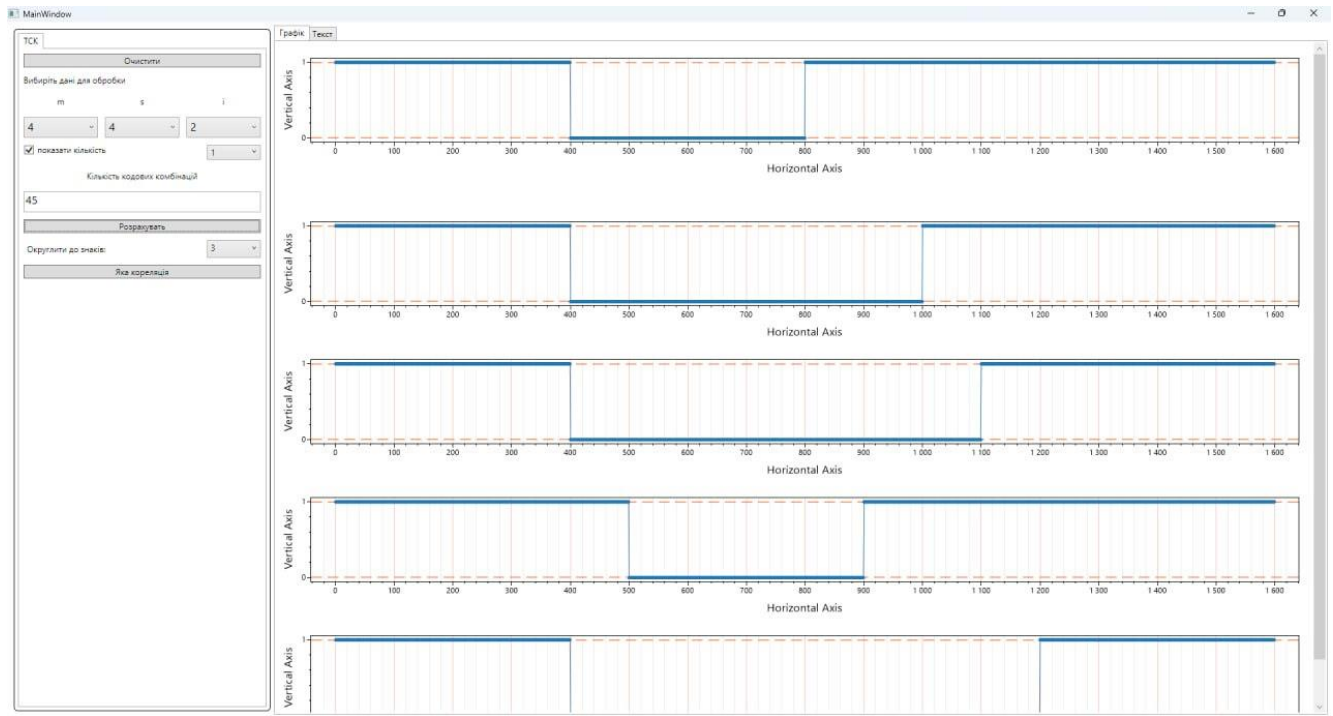
Кільдішев В.Й.

Стайкуца С.В.

Дунаєва В. В.

ДОДАТОК В

ІНТЕРФЕЙС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ТАЙМЕРНИХ СИГНАЛІВ



MainWindow

Графік Текст

Очистити

Вибір даних для обробки:

m: 4 s: 4 i: 2

☒ показати кількість

Кількість кодових комбінацій: 45

Розрахувати

Яка кореляція

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1,000	0,856	0,745	0,655	0,577	0,667	0,545	0,447	0,364	0,333	0,234	0,149	0,000	-0,078	-0,333
2	0,856	1,000	0,870	0,764	0,674	0,856	0,709	0,592	0,493	0,545	0,418	0,313	0,234	0,127	-0,078
3	0,745	0,870	1,000	0,878	0,775	0,745	0,870	0,733	0,618	0,745	0,592	0,467	0,447	0,313	0,149
4	0,655	0,764	0,878	1,000	0,882	0,655	0,764	0,878	0,746	0,655	0,764	0,618	0,655	0,493	0,364
5	0,577	0,674	0,775	0,882	1,000	0,577	0,674	0,775	0,882	0,577	0,674	0,775	0,577	0,674	0,577
6	0,667	0,856	0,745	0,655	0,577	1,000	0,856	0,745	0,655	0,667	0,545	0,447	0,333	0,234	0,000
7	0,545	0,709	0,870	0,764	0,674	0,856	1,000	0,870	0,764	0,856	0,709	0,592	0,545	0,418	0,234
8	0,447	0,592	0,733	0,878	0,775	0,745	0,870	1,000	0,878	0,745	0,870	0,733	0,745	0,592	0,447
9	0,364	0,493	0,618	0,746	0,882	0,655	0,764	0,878	1,000	0,655	0,764	0,878	0,655	0,764	0,655
10	0,333	0,545	0,745	0,655	0,577	0,667	0,856	0,745	0,655	1,000	0,856	0,745	0,667	0,545	0,333
11	0,234	0,418	0,592	0,764	0,674	0,545	0,709	0,870	0,764	0,856	1,000	0,870	0,856	0,709	0,545
12	0,149	0,313	0,467	0,618	0,775	0,447	0,592	0,733	0,878	0,745	0,870	1,000	0,745	0,870	0,745
13	0,000	0,234	0,447	0,655	0,577	0,333	0,545	0,745	0,655	0,667	0,856	0,745	1,000	0,856	0,667
14	-0,078	0,127	0,313	0,493	0,674	0,234	0,418	0,592	0,764	0,545	0,709	0,870	0,856	1,000	0,856
15	-0,333	-0,078	0,149	0,364	0,577	0,000	0,234	0,447	0,655	0,333	0,545	0,745	0,667	0,856	1,000
16	0,333	0,389	0,447	0,509	0,577	0,333	0,389	0,447	0,509	0,333	0,389	0,447	0,333	0,389	0,333
17	0,078	0,164	0,244	0,323	0,405	0,389	0,455	0,522	0,595	0,389	0,455	0,522	0,389	0,455	0,389
18	-0,149	-0,035	0,067	0,163	0,258	0,149	0,244	0,333	0,423	0,447	0,522	0,600	0,447	0,522	0,447
19	-0,364	-0,221	-0,098	0,016	0,126	-0,073	0,051	0,163	0,270	0,218	0,323	0,423	0,509	0,595	0,509
20	-0,577	-0,405	-0,258	-0,126	0,000	-0,289	-0,135	0,000	0,126	0,000	0,135	0,258	0,289	0,405	0,577
21	-0,509	-0,595	-0,423	-0,270	-0,126	-0,509	-0,323	-0,163	-0,016	-0,218	-0,051	0,098	0,073	0,221	0,364
22	-0,447	-0,522	-0,600	-0,423	-0,258	-0,447	-0,522	-0,333	-0,163	-0,447	-0,244	-0,067	-0,149	0,035	0,149
23	-0,389	-0,455	-0,522	-0,595	-0,405	-0,389	-0,455	-0,522	-0,323	-0,389	-0,455	-0,244	-0,389	-0,164	-0,078
24	-0,333	-0,389	-0,447	-0,509	-0,577	-0,333	-0,389	-0,447	-0,509	-0,333	-0,389	-0,447	-0,333	-0,389	-0,333
25	-1,000	-0,856	-0,745	-0,655	-0,577	-0,667	-0,545	-0,447	-0,364	-0,333	-0,234	-0,149	0,000	0,078	0,333
26	-0,856	-1,000	-0,870	-0,764	-0,674	-0,856	-0,709	-0,592	-0,493	-0,545	-0,418	-0,313	-0,234	-0,127	0,078
27	-0,745	-0,870	-1,000	-0,878	-0,775	-0,745	-0,870	-0,733	-0,618	-0,745	-0,592	-0,467	-0,447	-0,313	-0,149
28	-0,655	-0,764	-0,878	-1,000	-0,882	-0,655	-0,764	-0,878	-0,746	-0,655	-0,764	-0,618	-0,655	-0,493	-0,364
29	-0,577	-0,674	-0,775	-0,882	-1,000	-0,577	-0,674	-0,775	-0,882	-0,577	-0,674	-0,775	-0,577	-0,674	-0,577
30	-0,667	-0,856	-0,745	-0,655	-0,577	-1,000	-0,856	-0,745	-0,655	-0,667	-0,545	-0,447	-0,333	-0,234	0,000
31	-0,545	-0,709	-0,870	-0,764	-0,674	-0,856	-1,000	-0,870	-0,764	-0,856	-0,709	-0,592	-0,545	-0,418	-0,234
32	-0,447	-0,592	-0,733	-0,878	-0,775	-0,745	-0,870	-1,000	-0,878	-0,745	-0,870	-0,733	-0,745	-0,592	-0,447
33	-0,364	-0,493	-0,618	-0,746	-0,882	-0,655	-0,764	-0,878	-1,000	-0,655	-0,764	-0,878	-0,655	-0,764	-0,655
34	-0,333	-0,545	-0,745	-0,655	-0,577	-0,667	-0,856	-0,745	-0,655	-1,000	-0,856	-0,745	-0,667	-0,545	-0,333
35	-0,234	-0,418	-0,592	-0,764	-0,674	-0,545	-0,709	-0,870	-0,764	-0,856	-1,000	-0,870	-0,856	-0,709	-0,545
36	-0,149	-0,313	-0,467	-0,618	-0,775	-0,447	-0,592	-0,733	-0,878	-0,745	-0,870	-1,000	-0,745	-0,870	-0,745
37	0,000	-0,234	-0,447	-0,655	-0,577	-0,333	-0,545	-0,745	-0,655	-0,667	-0,856	-0,745	-1,000	-0,856	-0,667

ТКК

Очистити

Вибрати дані для обробки

m

s

i

4

4

2

☒ показати кількість

1

Кількість кодових комбінацій

45

Розрахувати

Яка кореляція

Графік

Текст

0: 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 1

1: 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0

2: 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 1

3: 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0

4: 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1

5: 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0

6: 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 1

7: 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0 0

8: 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1

9: 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0

10: 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1

11: 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0

12: 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1

13: 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0

14: 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1

15: 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0

16: 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1

17: 0 0 0 0 0 1 1 1 1 1 1 1 0 0 0 0

18: 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1

19: 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0

20: 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1

21: 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0

22: 1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1

23: 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0

24: 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1

25: 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0

26: 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1

27: 0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0

28: 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1

29: 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0

30: 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0

31: 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1

32: 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0

33: 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

34: 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0

35: 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1

36: 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

37: 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1

38: 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

39: 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1

40: 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0

24°C

Mostly cloudy

Пошук

УКР

100%

14:45

27.08.2026